





Página Datos Editoriales



Índice

Presentación. <i>Por Mario Gerlero</i>	12
La Sociedad De La Información No Resigna La Localización. <i>Por Corina Iuale</i>	14
Introducción: los orígenes del encuentro, la convergencia de grupos de investigación	19
Conferencia de apertura a cargo del Prof. Dr. Fernando Barrio	21
COMITÉ ACADÉMICO	25
Equipo de recepción de trabajos, gestión y edición.	26
Primera Parte	27
Presentación: La Inteligencia Artificial Frente al Derecho. Reflexiones sobre la importancia del eje del encuentro y sus discusiones. <i>Por Ernesto Liceda</i>	27
Capítulo 1. Planteos generales en el uso de la Inteligencia Artificial	36
INTELIGENCIA ARTIFICIAL: UNA DEFINICIÓN ENGAÑOSA. <i>Por Roberto Nelson Bugallo</i>	37
Resumen	
...Y El hombre creó a los dioses a su imagen y semejanza...	
La irrupción de las tecnologías digitales	
La apropiación del lenguaje	
La inteligencia artificial	
La falacia de la asimilación	
Bibliografía	
LIBERTAD DE EXPRESIÓN E INTELIGENCIA ARTIFICIAL EN LA RED. <i>Por Manuel Larrondo y Nicolás Mario Grandi</i>	44
Resumen:	
Introducción	
la y la moderación de contenido	
A modo de cierre abierto	
Bibliografía:	
CIBERTOTALITARISMO. UN EXAMEN DE LA IDEOLOGÍA “WOKE/ CANCEL CULTURE” <i>Por Mario S. Gerlero</i>	51
COMO NUEVO PARÁMETRO DE PRÁCTICAS EN EL CAMPO JURÍDICO.	

Resumen:

El uso de la tecnología digital como problemática socio-jurídica

El “ecosistema tecno-cultural”: de la ciber-militancia a la cancelación del debate

La cultura de la cancelación y la legitimación político - administrativa

Un resultado previsible: el “cibertotalitarismo”

Bibliografía:

LA ERA DE LOS ALGORITMOS ¿ENEMIGOS O ALIADOS?. *Por Ariadna Luján Martínez y Francisca Ojeda Campos* 66

Resumen

Introducción

Desarrollo

Conclusión

Bibliografía

Capítulo 2 La Inteligencia Artificial y su aplicación en situaciones problemáticas 72

LA INTELIGENCIA ARTIFICIAL AL SERVICIO DEL MARKETING LÍMITES AL TRATAMIENTO DE DATOS PERSONALES. *Por María de los Ángeles Tedesco* 73

Resumen:

Introducción: marketing tecnológico y minería de datos

El consentimiento y el tratamiento de datos personales

El principio de finalidad como límite

Conclusión

Bibliografía

SISTEMAS DE RECONOCIMIENTO FACIAL, UNA PREOCUPACIÓN PARA LOS DERECHOS HUMANOS. *Por Lucas Ezequiel Costabel, Mauren Belén Guiretti y Sol Iara Raschkovan* 81

Resumen

Introducción

Desarrollo

Conclusión

Bibliografía

LA UTILIZACIÓN DE INTELIGENCIA ARTIFICIAL EN EL DIAGNÓSTICO DE ENFERMEDADES. ESPECIAL CONSIDERACIÓN AL CASO DEL COVID-19. *Por Ana V. Visconti* 87

Resumen

Introducción

Opacidad de los Algoritmos

Secreto Empresarial y Derecho a la Información de los Pacientes

Comentario Final

Bibliografía

**LA MUTABILIDAD DEL ORDEN PÚBLICO INTERNACIONAL CUANDO CONCORRE CON 92
LA INTELIGENCIA ARTIFICIAL DECISORIA.** *Por Corina Andrea Iuale*

Resumen:

Introducción

Diversos tipos de Sistemas Expertos Jurídicos

La Inteligencia Artificial en la creación del Derecho. El Orden Público Internacional.

Conclusiones

Bibliografía

APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO JURÍDICO. *Por Carlos 97
Martín Aznar*

Resumen

Introducción

Inteligencia Artificial

Inteligencia Artificial Y Derecho

Conclusión

Bibliografía

**RESPONSABILIDAD PENAL DEL PROGRAMADOR Y LA EMPRESA DE INTELIGENCIA 104
ARTIFICIAL.** *Por Nicolás Mario Grandi*

Resumen:

Introducción

Diferencias entre la IA y los productos convencionales

Conclusión

Bibliografía:

**CONSIDERACIONES SOBRE LA ASIGNACIÓN DE RESPONSABILIDAD PENAL A LA 110
INTELIGENCIA ARTIFICIAL.** *Por Federico Daniel Arrué*

Resumen:

Introducción y Esquema del Trabajo

Argumentos a favor del establecimiento de la Responsabilidad Penal de la Inteligencia Artificial.

Los Propósitos De La Pena A La Inteligencia Artificial Desde Las Distintas Teorías

Evolución Social Y Cambios De Paradigma

Palabras Finales

Bibliografía

**Segunda Parte. Presentación: Digitalización y Derecho Procesal Electrónico. 117
Reflexiones sobre la importancia del eje del encuentro y sus discusiones.** *Por José
María Lezcano*

Capítulo 3. Algunos enunciados sobre las Tecnologías Digitales en el Proceso Judicial 121

TECNOLOGÍAS DIGITALES Y PROCESO JUDICIAL. UNA COMPLEJA RELACIÓN 122

ENTRE INSTRUMENTOS Y PRINCIPIOS. *Por José María Lezcano*

Resumen
Introducción
El problema: las tensiones en el proceso de cambio
La Tecnología desde la Filosofía y las Ciencias Sociales
Los llamados principios del Derecho Procesal Electrónico
A modo de cierre
Bibliografía

LA TRANSFORMACIÓN DEL PROCESO JUDICIAL: DEL IUDEX A LA INTELIGENCIA ARTIFICIAL. *Por Andrés S. Díaz Etulain y Javier M. Yabante* 131

Resumen
Introducción
Aproximación al concepto de Inteligencia Artificial
Etapas del desarrollo de la Inteligencia Artificial
Conclusión
Bibliografía citada.

DERECHO PENAL Y LAS NUEVAS TECNOLOGÍAS: el uso de la inteligencia artificial. 136
Por Matías Nicolás Bares Menna

Resumen
Las nuevas Tecnologías de la Información y Comunicación (TIC)
La utilización de la Inteligencia Artificial en el Derecho Penal actual
Bibliografía:

EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL: UNA MIRADA A LA LUZ DEL DEBER DE MOTIVACIÓN Y DE LA AVERIGUACIÓN DE LA VERDAD SOBRE LOS HECHOS DEL CASO. *Por Pablo Antonio Molina* 142

Resumen
Introducción
Inteligencia Artificial y Algoritmos
Verdad de los hechos y motivación
Conclusiones
Bibliografía

LA APLICABILIDAD DE MACHINE LEARNING EN LOS JUZGADOS DE ARGENTINA ¿UNA POTENCIAL HERRAMIENTA EN EL ACCESO A LA JUSTICIA?. *Por Elian Facundo Yorlano* 149

Resumen
Introducción
Bibliografía

DIGITALIZACIÓN DEL PODER JUDICIAL, EL DESAFÍO DE CUIDAR LA DIGNIDAD. *Por* 156

Ernesto Liceda y Marina Flammini

Resumen
Introducción y desarrollo
Primeras conclusiones
Bibliografía

Capítulo 4. Las Tecnologías Digitales en los Procesos de Administración de Justicia 162

PANDEMIA: TIERRA FÉRTIL PARA LA INSTAURACIÓN DE LA FILOSOFÍA DIGITAL EN EL ÁMBITO JUDICIAL. *Por María Fernanda Díaz* 163

Resumen
Introducción
Estado de cosas: desafíos actuales para la humanidad
El expediente electrónico como garantía de la tutela judicial efectiva
Conclusiones: ¿temporalidad o sostenibilidad?
Bibliografía

IMPLICANCIAS PRÁCTICAS DE LA RESOLUCIÓN 10/20 DICTADA POR EL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES EN EL RÉGIMEN DE NOTIFICACIONES. *Por Julieta Melendi* 169

Resumen
Introducción

Resumen
Introducción
Resumen

EL SISTEMA DE UDRP DE ICANN APLICADO COMO MODELO A CONFLICTOS DE COMERCIO ELECTRÓNICO. *Por Rolando Joaquín Ortega Hernandez* 177

Resumen
Introducción
Desarrollo
Conclusiones
Bibliografía

CRÓNICA DE UN RECHAZO ANUNCIADO, A Propósito del Per Saltum de Google. *Por Mariel Alejandra Suárez* 184

Resumen
Introducción
De la evidencia digital y su tratamiento
Del trabajo de los peritos informáticos forenses y la presentación de la evidencia digital ante el juez
A propósito del caso Google – algunas referencias sobre la prueba anticipada
De los análisis que no se efectuaron a modo de conclusión:
Bibliografía

LA PRUEBA EN LAS OPERACIONES CON CRIPTOACTIVOS. *Por Fernando O. Branciforte* 192

Resumen
Introducción
Conceptos Básicos
Actividad Probatoria
Transacción Realizada En Blockchain Pública
Transacción Realizada En Blockchain Privada
Conclusión

IMPACTOS PENALES Y CIVILES DEL RANSOMWARE. *Por María José Quintana Dourado* 197

Resumen
Introducción
Qué es, y a quiénes afecta un ataque de ransomware
Qué delitos encierra el ransomware?
Responsabilidad de las víctimas frente a terceros
Un desafío para todos los actores sociales
Bibliografía

Capítulo 5. TERCERA PARTE: Enseñanza e investigación en Derecho y Nuevas Tecnologías 203

por Corina Andrea Iuale

INTERACCIÓN DEL DERECHO Y LAS TECNOLOGÍAS: RETO PARA UNA NUEVA SOCIEDAD CON CONCIENTIZACIÓN DIGITAL. *Por Edda Karen Céspedes Babilón* 205

Resumen
Introducción
Problema
Objetivo
Marco teórico
 Internet
Tecnologías de la información y comunicaciones - TIC
Ciberdelitos
Ciberseguridad
Inteligencia artificial
Relevancia de la interacción del derecho y el avance tecnológico en el siglo xxi
Derecho informático
La importancia actual del teletrabajo
El crecimiento de los ciberdelitos
La redes sociales, la privacidad y violencia digital
La disrupción de la Inteligencia Artificial (IA)
Importancia de la protección de datos personales y la ciberseguridad

Protección de datos personales
 Importancia de la ciberseguridad
 Aportes e importancia prioritaria de la concientización digital
 Bibliografía

FORMANDO A LOS PROFESIONALES DEL ¿FUTURO?. EXPERIENCIAS PRÁCTICAS DE FORMACIÓN. *Por Juan M. Brussino K. y Ana E. Lambrecht* 220

Resumen
 Introducción
 El Derecho Informático como asignatura
 Actividad de investigación
 Conclusión
 Bibliografía

¿SON LAS NUEVAS TECNOLOGÍAS UNA NUEVA FORMA DE VER, ENTENDER Y ENSEÑAR EL DERECHO?. *Por Fernando O. Branciforte* 226

Resumen:
 ¿qué son las nuevas tecnologías?
 Su influencia en el derecho
 ¿una nueva forma de analizar y transmitir el derecho?
 Conclusión

LA ENSEÑANZA DEL DERECHO EN FORMA VIRTUAL: DESCRIPCIÓN Y ANÁLISIS DE LO SUCEDIDO DURANTE LA PANDEMIA. *Por Marcos Fernández Peña y Martina Santillán* 232

Resumen
 Introducción
 Resultados de la encuesta.
 Enseñanza Práctica del Derecho.
 Relación docente- estudiante y Relación entre pares.
 Experiencias Personales.
 Conclusión
 Referencias Bibliográficas

Capítulo 6 La Tecnología en la Investigación y en la Experiencia Práctica 238

EL CATÁLOGO DE DERECHOS DIGITALES EN LA LEGISLACIÓN ESPAÑOLA Y EUROPEA. *Por Wilma Arellano Toledo* 223

Resumen:
 Sobre los nuevos Derechos Digitales en la normativa europea
 Los nuevos Derechos Digitales en la normativa española
 Bibliografía

DOS SENTENCIAS INTERESANTES. *Por Roberto Nelson Bugallo* 248

Resumen:

Injurias por Twitter

A) Nuevas figuras productoras de daño:

B) Dificultades procesales:

C) Cuestiones de competencia:

N.n. c/facebook s/habeas data

EL PASADO (¿QUE NOS PERSIGUE?) EN TIEMPOS DE INTERNET. *Por Martina Andrea Gutiérrez* 255

Resumen

Introducción

Derecho al Olvido en Internet, ¿qué es?

El fallo Belén Rodríguez.

Fallo Natalia Denegri

Cuál es la importancia del Fallo Denegri

Conclusiones

Bibliografía consultada

RESPONSABILIDAD CIVIL DE LAS PLATAFORMAS DIGITALES FRENTE AL CONSUMIDOR. *Por Florencia Romina Gianfelici* 261

Resumen

Introducción

Los casos en análisis

El fallo "Kosten". (Kosten, Esteban c/ Mercado Libre SRL, 2018)

El fallo "Mercado Libre". (Mercado Libre SRL c/ Dirección de Defensa del Consumidor y Lealtad, 2020).

El diálogo

Conclusión

Referencias

NÓMADAS DIGITALES. *Por Verónica S. Arizcuren* 271

Resumen

Introducción: la Revolución 4.0

¿qué es el trabajo nómada digital?

Tipos de trabajadores

Legislación aplicable. La negociación colectiva

Bibliografía

IMPRESIÓN 3D INTELIGENTE Y DESEMPLEO CON SUS RESPECTIVAS CONSECUENCIAS EN EL DERECHO. *Por Manuel Martín Pino Estrada* 277

Resumen:

Introducción

La impresión 3D

Impresión 3D y desempleo

La impresión 3D en otras áreas del Derecho

En la cuestión de pruebas

En los Derechos de Autor

Conclusiones

Referencias

RETOS DE LA REGULACIÓN ESTATAL DE LA DESINFORMACIÓN EN EL CIBERESPACIO E INTERNET. *Por Ernesto Ángeles Guerrero*

283

Resumen:

Introducción

Elementos de la desinformación y las opciones regulativas del Estado

Bibliografía citada

Presentación

En el momento de hacer la introducción a este texto coral, que surge del intercambio de profesionales comprometidos con la cultura digital en el campo jurídico, hemos perdido una referente de nuestro trabajo.

La hacedora del GECSI-UNLP nos dejó, pero antes de su partida nos permitió ser colmados por su calidad como personal y por su aporte institucional. Si bien entiendo perfectamente que esta situación da lugar a una circunstancia de introspección personal, también creo que es una instancia que confirma el hecho de seguir cumpliendo con la promesa de expandir su legado.

Como nuevo Director de este grupo de estudios secundo y confirmo, con esta presentación, la tarea de compilar experiencias de diferentes colegas de distintas áreas con el fin persistir en la promoción de las nuevas tecnologías en las facultades de Ciencias Jurídicas y de Derecho como, además, colaborar con la creación de ecosistemas de integrabilidad digital. Objetivos ambiciosos pero posibles de realización a partir de diferentes afanes y ejercicios. En este caso, con notable resultado, que queda plasmado en una compilación de una pluralidad de voces; un texto producto del esfuerzo y diligencia a cargo de tres colegas acreditados en la difusión del presente tema: José María Lezcano, Ernesto Liceda y Corina Iuale.

Bajo el designio de la fundadora GECSI-UNLP, y en este trabajo, se potencia la fluida intervención de cada uno de los integrantes del equipo, sus becarios y sus tesisistas con el firme propósito de lograr expandir la influencia de la cultura digital en el árido campo jurídico. Un ejemplo de lo expuesto, insisto, es la razón del presente texto cuando refiere a las distintas miradas y tópicos alternativos en la diversidad de matices de la cultura digital presente en las Instituciones Jurídicas; trabajo en equipo

que, con una mirada crítica, continúa explorando y profundizando nuevas aristas de los temas que se presentan.

Texto este que remarca la necesidad de continuar con una larga labor de peregrinar por las áreas jurídicas para consolidar, fomentar e incrementar sistemas digitalizados lo más avanzado posible en esa temática; asimismo insiste extender la difusión con el firme propósito de la incorporación de esa cultura digital en las prácticas de gestión cotidianas y en la consideración de la socialización y formación de los operadores del derecho. Toda una oportunidad para construir una sociedad más dinámica y menos burocrática.

Dudas no caben que, con actividades como esta encuentro, se apunta a insistir en el camino de la calidad institucional siempre con la mira puesta en el disenso y las alternativas jurídicas y de gestión administrativa cotidiana.

Este libro, siguiendo la fuerza que ponía la Profesora Noemí Olivera en el proyecto de habilitar las técnicas de información y comunicación en el campo jurídico, está profundamente dedicado a ella y a aquellas personas que con su contribución diaria impulsan miradas alternativas y propuestas de cambio en el sistema jurídico/judicial.

A Noemí. Gracias.

Prof. Mario S. Gerlero

Director

GECSI-UNLP

LA SOCIEDAD DE LA INFORMACIÓN NO RESIGNA LA LOCALIZACIÓN

Por Corina Andrea Iuale

En el presente voy a poner en vigencia un tema sobre el cual se ha escrito mucho cuando, hace ya largo tiempo desde el derecho nos adentramos en los problemas que al mismo le presentaba la sociedad de la información.

La prevención que estoy haciendo refiere a la existencia de los ordenamientos jurídicos de los Estados y a sus fronteras. Cuántos artículos de aquella primera época comenzaban con alguna referencia a la dudosa existencia de las fronteras en internet! Muchas de esas reflexiones se fundaban en la circunstancia por la que con un click, y de modo casi imperceptible se vinculaba la cuestión con otro país el ordenamiento jurídico de otro país, como es el caso de los contratos internacionales celebrados por medios electrónicos. La referencia a esta cuestión tiene por objeto resaltar que más allá del medio empleado, no estamos –aún- viviendo en un mundo virtual, sino en un mundo real en el que las situaciones jurídicas y las relaciones deben anclarse a un lugar geográfico, el cual nos va a indicar qué ordenamiento jurídico alcanzará a una situación o relación jurídica en particular.

En cuanto al domicilio, la cuestión del domicilio físico en la sociedad de la información recepta cuestiones que van más allá del derecho privado y alcanza al derecho internacional privado. Ello es así, por cuanto en el contexto del derecho internacional privado perdura la necesidad de la localización de la relación jurídica en el campo de la problemática de la aplicación del derecho extranjero en tanto la norma de derecho internacional privado así lo indique, y son diversas las situaciones en las que la relación jurídica se rige por el derecho del domicilio de alguna de las partes.

El domicilio físico, es un punto de conexión relevante y no se halla superado por el domicilio electrónico, claro está que la importancia del domicilio electrónico resulta de

interés pero más como un modo cierto de comunicación que para satisfacer la necesidad de la localización de las situaciones y relaciones jurídicas nacionales e internacionales.

El art. 2652 CCyC establece para la determinación del derecho aplicable en materia contractual internacional, que en los casos en los que las partes no pactan el derecho aplicable, el contrato se rige por las leyes y usos del país del lugar de cumplimiento; pero que si el lugar de cumplimiento no estuviere designado o no surgiere de la naturaleza de la relación, se entenderá que lugar de cumplimiento es el del domicilio actual del deudor de la prestación más característica del contrato¹.

Asimismo, en los contratos de consumo el art. 2655, establece que el derecho aplicable es el que corresponde al Estado del domicilio del consumidor en los caso que expresamente la norma prevé².

Podría afirmarse que en ciertos enfoques que se van haciendo en el sofisticado tema de la relación del derecho y las tecnologías, se abordan temas vinculados a estas relaciones sin una ubicación normativa, como si estuviéramos sometidos todos a las mismas leyes, algo así como un mundo en el que rigen las mismas reglas para todos, negando con ello lo innegable, como es la existencia de los límites de cada ordenamiento jurídico.

El derecho sigue necesitando localizar la cuestión fáctica dentro de un cierto espacio físico para determinar el ordenamiento jurídico en el cual queda comprendida, así como para poder determinar además si la cuestión es nacional de derecho privado o internacional del

-
- 1 Código Civil y Comercial, artículo 2652: Determinación del derecho aplicable en defecto de elección por las partes. En defecto de elección por las partes del derecho aplicable, el contrato se rige por las leyes y usos del país del lugar de cumplimiento. Si no está designado, o no resultare de la naturaleza de la relación, se entiende que lugar de cumplimiento es el del domicilio actual del deudor de la prestación más característica del contrato. En caso de no poder determinarse el lugar de cumplimiento, el contrato se rige por las leyes y usos del país del lugar de celebración. La perfección de los contratos entre ausentes se rige por la ley del lugar del cual parte la oferta aceptada
 - 2 Código Civil y Comercial, artículo 2655: Derecho aplicable. Los contratos de consumo se rigen por el derecho del Estado del domicilio del consumidor en los siguientes casos: a) si la conclusión del contrato fue precedida de una oferta o de una publicidad o actividad realizada en el Estado del domicilio del consumidor y éste ha cumplido en él los actos necesarios para la conclusión del contrato; b) si el proveedor ha recibido el pedido en el Estado del domicilio del consumidor; c) si el consumidor fue inducido por su proveedor a desplazarse a un Estado extranjero a los fines de efectuar en él su pedido; d) si los contratos de viaje, por un precio global, comprenden prestaciones combinadas de transporte y alojamiento. En su defecto, los contratos de consumo se rigen por el derecho del país del lugar de cumplimiento. En caso de no poder determinarse el lugar de cumplimiento, el contrato se rige por el derecho del lugar de celebración.

derecho privado. Si se tratara de un caso internacional, serán de aplicación las normas cuya aplicación indique la norma de derecho internacional privado.

Puede afirmarse que la localización para el derecho internacional privado puede estar cambiando pero nunca que ella pueda faltar.

La Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, refiere a cuestiones de índole geográfica cuando se ocupa de la ubicación de las partes. En el artículo 6³ establece pautas vinculadas a la ubicación de las mismas estableciendo que un lugar no constituye un establecimiento por el mero hecho de que sea el lugar en el que se hallen ubicados el equipo y la tecnología que sirvan de soporte para el sistema de información utilizado por una de las partes para la formación de un contrato; o donde otras partes puedan obtener acceso a dicho sistema de información 5⁴. El mero hecho de que una parte haga uso de un nombre de dominio o de una dirección de correo electrónico vinculados a cierto país no crea la presunción de que su establecimiento se encuentra en dicho país.

Asimismo, no podemos sortear la mención del inciso 5 del artículo 6, en cuanto establece una regla realmente novedosa que dispone que el mero hecho de que una parte haga uso de un nombre de dominio o de una dirección de correo electrónico vinculados a cierto país

-
- 3 Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, artículo 6. Ubicación de las partes 1. Para los fines de la presente Convención, se presumirá que el establecimiento de una parte está en el lugar por ella indicado, salvo que otra parte demuestre que la parte que hizo esa indicación no tiene establecimiento alguno en ese lugar. 2. Si una parte no ha indicado un establecimiento y tiene más de un establecimiento, su establecimiento a efectos de la presente Convención será el que tenga la relación más estrecha con el contrato pertinente, habida cuenta de las circunstancias conocidas o previstas por las partes en cualquier momento antes de la celebración del contrato o al concluirse éste. 3. Si una persona física no tiene establecimiento, se tendrá en cuenta su lugar de residencia habitual. 4. Un lugar no constituye un establecimiento por el mero hecho de que sea el lugar: a) donde estén ubicados el equipo y la tecnología que sirvan de soporte para el sistema de información utilizado por una de las partes para la formación de un contrato; o b) donde otras partes puedan obtener acceso a dicho sistema de información. 5. El mero hecho de que una parte haga uso de un nombre de dominio o de una dirección de correo electrónico vinculados a cierto país no crea la presunción de que su establecimiento se encuentra en dicho país. 5 Artículo 7. Requisitos de información Nada de lo dispuesto en la presente Convención afectará
 - 4 Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, artículo 5: Interpretación 1. En la interpretación de la presente Convención se tendrán en cuenta su carácter internacional y la necesidad de promover la uniformidad en su aplicación y de velar por la observancia de la buena fe en el comercio internacional. 2. Las cuestiones relativas a las materias que se rigen por la presente Convención que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se inspira su régimen o, en su defecto, de conformidad con la ley aplicable en virtud de las normas de derecho internacional privado.

no crea la presunción de que su establecimiento se encuentra en dicho país. De este modo, la Convención parece asumir un hecho de la realidad que ha demostrado que la simple asignación de nombres de dominio y de direcciones de correo electrónico no siempre proveen lazos confiables, fiables de efectiva conexión con determinado Estado⁵.

El domicilio a los efectos de la determinación de la jurisdicción

En los autos Pérez Morales, Gonzalo Martín c. Booking.com Argentina SRL y otros s/ ordinario⁶ el actor habría contratado a través del sitio www.booking.com.ar el servicio de hospedaje mediante sendas reservas efectuadas respecto de dos hoteles ubicados en España y Francia. Tal reserva había sido abonada mediante la tarjeta de crédito del accionante y, posteriormente, éste habría requerido la cancelación de dicha operación y la restitución de los importes abonados, lo que habría sido denegado por la codemandada Booking.com Argentina S.R.L.

De la sentencia de la Cámara Nacional de Apelaciones en lo Comercial, se extrae que el caso trata de una relación de consumo en la que resulta aplicable el Código Civil y Comercial en cuanto a las disposiciones de Derecho Internacional Privado, dada la inexistencia de tratado internacional que regule la cuestión. La particularidad del caso es que pone de resalto que si bien existe la dificultad para elegir una pauta válida determinante de la jurisdicción competente por ser un contrato celebrado en el ciberespacio, en el que las partes tienen una dirección electrónica virtual con un sufijo geográfico (ar, br, pl, fr, es, etc.), continúa teniendo actualidad el punto de conexión domicilio real aún cuando no coincida con el domicilio virtual ya que el real ofrece un principio perenne de localización, que en el caso resulta ser el domicilio de la excepcionante (la demandada) fijado en la Av. L. Alem 928, piso 7°, of. 721, CABA. Se indica que no resulta relevante la ubicación del server mediante el cual se logra la conexión a la red (Ámsterdam, Países Bajos), o la localización física de sus computadoras

5 FELDSTEIN DE CÁRDENAS, Sara y SCOTTI, Luciana La convención sobre utilización de las comunicaciones electrónicas en los contratos internacionales: un avance hacia la armonización legislativa en materia de contratación electrónica Revista Científica de UCES Vol. XI N° 1 - Otoño 2007

http://dspace.uces.edu.ar:8180/jspui/bitstream/123456789/198/1/La_convenci%C3%B3n_sobre_utilizaci%C3%B3n.pdf

6 C(CNCom)(SalaC) Fecha: 10/08/2017 Partes: Publicado en: LA LEY 26/09/2017, 26/09/2017, 10 Cita Online: AR/JUR/53519/2017

—como pregona la excepcionante—, pues si estos criterios fueran aceptados, el deudor en caso de ser perseguido podría modificar a distintos Estados la ubicación de los servidores y/o el punto de conexión a la red a su propio albedrío, dificultando la posibilidad de ser sometido a justicia alguna, generando inseguridad jurídica en la relación de comercio electrónico en cuestión. Y aún cuando pueda resultar difícil y hasta casi imposible localizar el domicilio del demandado, en tanto existan elementos suficientes que lo vinculen con nuestro país, se ha de preconizar una interpretación amplia del concepto, por el que los jueces argentinos podrían asumir jurisdicción internacional en virtud del llamado foro de necesidad cuando el cierre del caso pudiera producir una efectiva denegación internacional de justicia. (art. 2602 Cód. Civ. y Com. de la Nación).

El abordaje de la localización, y sin perjuicio de lo expuesto precedentemente, nos indica que debemos detenernos en una regla incorporada en el CCyC que podría ser interpretada como un modo de flexibilización pero no lo es a los efectos de la necesidad de la localización: me estoy refiriendo a la regla por la que, cuando el caso tiene lazos poco relevantes con el derecho designado por la norma ese derecho no debe ser aplicado. Se trata de una situación de excepción, en la que se va a tener en consideración la relevancia del conjunto de las circunstancias de hecho con vínculos muy estrechos con el derecho de otro Estado, cuya aplicación resulta previsible y bajo cuyas reglas la relación se ha establecido válidamente, artículo 2597⁷.

Para finalizar: La negación de la vigencia de la localización, implica una liviana simplificación de los problemas jurídicos a resolver en la sociedad de la información.

7 Código Civil y Comercial, artículo 2597: Cláusula de excepción. Excepcionalmente, el derecho designado por una norma de conflicto no debe ser aplicado cuando, en razón del conjunto de las circunstancias de hecho del caso, resulta manifiesto que la situación tiene lazos poco relevantes con ese derecho y, en cambio, presenta vínculos muy estrechos con el derecho de otro Estado, cuya aplicación resulta previsible y bajo cuyas reglas la relación se ha establecido válidamente.

Introducción: los orígenes del encuentro, la convergencia de grupos de investigación. Conferencia de apertura a cargo del Prof. Fernando Barrio

En el marco de las múltiples enseñanzas que la experiencia de la Pandemia del Covid-19 nos viene dejando, habiendo transcurrido ya unos meses del Aislamiento Social Preventivo y Obligatorio (ASPO) y un entrenamiento intensivo en actividades a distancia (no presencial o virtual, sea cual sea el término que utilicemos para este modo de trabajo), la sincronía entre dos grupos de investigación de universidades públicas dió la posibilidad de realizar el encuentro de docentes, investigadores, graduados y estudiantes de Derecho y Tecnología. Hace algunos años atrás, ambos equipos de investigación, habíamos realizado el primer encuentro, presencial en aquel momento, en el Departamento de Derecho de la Universidad Nacional del Sur. En esta oportunidad, gracias a las circunstancias referidas y con las prácticas mediadas por herramientas de Tecnologías Digitales que viabilizan las maneras de “hacer desaparecer” lo más posible las distancias, concretamos en noviembre del año 2020 este nuevo encuentro sincrónico y a-sincrónico vía streaming.

El proceso fue iniciado con la convocatoria a la presentación de resúmenes y envío de comunicaciones de trabajo. Luego del pertinente referato del comité académico del encuentro, estas comunicaciones se complementaron por un video de autores y autoras que, estando disponible en línea fue el preludeo del encuentro realizado a través de una plataforma Zoom el día 2 de noviembre.

Así, en el marco de todas las crisis, incertidumbres y angustias de la Pandemia Covid-19, el encuentro del 2020 resultó una posibilidad de reencontrar los espacios de trabajo ya compartidos en diferentes foros, congresos, simposios y otros espacios académicos entre dos grupos de investigación de la UNLP y la UNS⁸. Iniciados por la profesora Noemí Olivera y la profesora Corina Iuale, ambas directoras de investigación de dos proyectos convergentes en temas, problemas y preocupaciones sobre el

8 Proyecto I+D J183: “Servicio de justicia y gestión en contexto de las tics: antecedentes, desarrollo, expansión y proyección de la digitalización en el servicio de justicia relacionada a los Derechos Humanos de cuarta generación”. Director: Prof. Dr. Mario Silvio Gerlero. GECSI-FJCyS-UNLP.

devenir jurídico y social del derecho y la Internet, la Sociedad de la Información, el Derecho Informático y otros aspectos que hace 10 años atrás motivaron el encuentro Jornada Derecho Informático, Bahía Blanca, UNS⁹.

Esta cierta agilidad en el uso de los sistemas streaming ayudó a que los permanentes desafíos que la tecnología presenta al derecho y las instituciones sociales y jurídicas puedan ser analizados, discutidos y estudiados en la horizontalidad que presentó el modelo de trabajo planteado. Esta modalidad resultó aceptada y aprovechada por los y las participantes para discutir sobre los comportamientos (o conductas) sociales y las posibles respuestas jurídicas, cuando ellos se encuentran mediados por tecnologías digitales. Claramente, estas discusiones incluyeron una necesaria búsqueda de la comprensión de los “comportamientos” tecnológicos que la Inteligencia Artificial (IA) nos trae como novedad para ser analizados “desde el”, “en el” o “frente al” Derecho. Consecuentemente, en su estudio se ponen en juego las discusiones sobre las clásicas teorías e Institutos Jurídicos que podrían llegar a dar respuesta a los

nuevos fenómenos socio jurídicos (¿o socio tecno jurídicos?). Cabe destacar que la horizontalidad que presentaron las discusiones entre investigadores e investigadoras, docentes y estudiantes de Derecho tuvo un rico valor agregado.

Para este encuentro, se propusieron tres ejes generales de trabajo: el primero convocando a trabajos, comunicaciones y producciones científicas sobre aspectos de la inteligencia artificial frente al derecho; el segundo sobre cuestiones vinculadas a la digitalización del Poder Judicial; y un tercero referido a la enseñanza e investigación en Derecho y Nuevas Tecnologías. En esta obra de compilación encontrarán las comunicaciones enviadas por los y las autoras al encuentro, así como los enlaces a los videos que formaron parte del material asincrónico. Estos videos, presentados con anterioridad al evento, funcionaron a modo de disparadores para abordar las comunicaciones enviadas y revisadas por el Comité Académico. En esta compilación, al iniciar cada parte de dos capítulos cada una, se presentan algunas consideraciones y conclusiones sobre los debates realizados en el encuentro sincrónico.

9 Enlace Youtube: [Jornada Derecho Informático - 23 08 10](https://www.youtube.com/watch?v=w3efx7XUAKk&t=263s) - <https://www.youtube.com/watch?v=w3efx7XUAKk&t=263s>

Conferencia de apertura a cargo del Prof. Dr. Fernando Barrio¹⁰

Unos párrafos aparte merece la apertura del encuentro, que estuvo a cargo del profesor Fernando Barrio. Este excelente colega y amigo, tituló su presentación “*El día de la marmota digital: la inteligencia artificial y la vuelta al fundamentalismo de la autorregulación*”¹¹. Su análisis, comenzó con un desarrollo de la situación desde una perspectiva histórica y cíclica de la relación derecho y tecnología. Inició su planteo a partir de la película clásica “El día de la marmota”, trayendo a colación las ideas de los años 90, donde los estudios del derecho y la tecnología, presentaban a esta última como una panacea, “la tecnología como solución a problemas que ni siquiera existían”. A partir de esta histórica mirada, presentó tanto discusiones desde una perspectiva teórica como ideológica. En ese marco, explicó las discusiones entre la escuela de Chicago, que entre sus referentes se encontraba Frank H. Easterbrook¹² respecto de la no regulación de las tecnologías, argumentando en contra de la noción de definir el ciberderecho como

¹⁰ Senior Lecturer in Business Law. Academic Lead Resident Futures Initiatives. Queen Mary University of London. f.barrio@qmul.ac.uk

¹¹ Enlace al video de la conferencia: <https://youtu.be/MYQengQclYs>

¹² Frank H. Easterbrook: “Cyberspace and the Law of the Horse”, Journal Article University Chicago Law School (1996)

una sección única de estudios jurídicos y litigios, por un lado, y la escuela de Harvard, desde la cual Lawrence Lessig¹³, plantea una necesaria mirada bajo la cual el derecho tenga algo que decir sobre estas innovaciones tecnológicas.

Este estado de discusión se mantuvo durante la primera década del siglo. Durante dicha etapa, explicó el profesor argentino de la University Queen Mary de Londres, las voces que más prosperaron en este punto fue la autorregulación. Esto estuvo sumido en una gran discusión ideológica y fuerte impacto en cómo debe ser el Derecho. En ellas, se puso en relieve una perspectiva subyacente que denomina “fundamentalismo tecnológico”, el cual se apoya en la creencia que la tecnología digital representa un bien tan superior, que de ninguna manera hay que tomar medida alguna que coarte su desarrollo”. A comienzos del siglo, el planteo era: “si regulamos, vamos a dar lugar a que no se desarrolle de forma cabal la tecnología”. Esta afirmación se apoya en una premisa no demostrada, y lo expresa el conferencista diciendo: “¿dónde está escrito que dejar que la tecnología se desarrolle por siempre, representa un bien para las personas o para la sociedad?”

¹³ Lawrence Lessig “The Law of the Horse: What Cyberlaw Might Teach”, 113 Harv. L. Rev. 501 (1999)

Esta posición, fue claramente apoyada por las empresas y diversas ONGs (la gran mayoría financiadas por empresas de tecnología) que frente a cada discusión sobre la posible regulación de tecnologías, se presentan en una defensa acérrima de la no intervención del derecho en el desarrollo de la tecnología o directamente la autorregulación, mayormente bajo las banderas de la “libertad de expresión”. De esta manera se produce una confusión entre la “tecnofilia” -una creencia del bien absoluto del desarrollo de la tecnología- con ser “tecnobobos” -la creencia de considerar que al tener un teléfono inteligente en el bolsillo, nos hace automáticamente más inteligentes a nosotros mismos-.

Estas discusiones de aquellos años, a más de dos décadas del inicio de esos planteos, permiten observar que aquellas proyecciones que se hacían sobre que el desarrollo tecnológico, por sí mismo iba a producir “mayor libertad, mayor libertad de expresión, mayor igualdad, menor discriminación, mayor equidad socio-económica... veamos cómo estamos hoy...”, bajo la cual se observa un fenómeno de gran expansión económica pero al mismo tiempo una disparidad de ingresos como no se ha conocido antes en la historia.

Al entrar directamente en las consideraciones sobre la Inteligencia Artificial (IA), Barrio marcó las diferencias entre machine learning y deep learning, marcando un elemento fundamental de su funcionamiento, como es la búsqueda de patrones. Esto es clave para la relación entre IA y el derecho porque el saber cómo funciona el algoritmo, una vez que se lo empieza a utilizar, es un conocimiento muy oscuro, a veces hasta para el propio creador de la IA. Este desconocimiento, sumado a la gran propensión a no contradecir el algoritmo, pone en situación muy compleja en relación a los roles y funciones de cada uno, piénsese el caso de usuarios como pueden ser un juez o un decisor.

En su descripción del problema, remarca que un aspecto de atención lo constituye nuevamente el impulso acrítico de esta tecnología, no sólo desde las empresas, sino también desde gran parte de la academia. Parece lógico considerar que el estado de situación que se refleja hoy (claramente distópico), consecuencias de la no regulación de la tecnología, o la autorregulación, puede resultar altamente peligroso si se propone el mismo camino sobre la IA puntualmente.

Entonces, continúa el profesor Barrio, se habla de principios éticos de la IA. Al entrar en este plano, se puede poner en

discusión la crítica al positivismo kelseniano, desde la cual es muy cuestionable la distinción entre moral y derecho, no obstante ello, más allá de la impureza del derecho, los principios éticos pueden estar o no, siempre y cuando se transformen en normas de derecho. Así, cuestiona el ímpetu en considerar únicamente los principios éticos de la IA, porque frente a ello aparece la pregunta: “¿dónde queda el derecho?”. Las evidencias muestran que la IA se está utilizando para decisiones jurídicas, trayendo en muchos casos problemas serios, entre otras cosas por la imposibilidad de verificación, sumado al desconocimiento, la opacidad del algoritmo, la imposibilidad de defensa y la violación de derechos fundamentales a diario a raíz del uso de IA. En este punto, las discusiones presentan una especie de resignificación o modificación del clásico “in dubio pro reo”, a favor de la tecnología, pues el enunciado sería “a no ser que se demuestre que la tecnología causa un daño, hay que dejarla que se desarrolle”. Este es el punto bajo el cual, parece que nos encontramos en el “Día de la marmota”: ya estuvimos acá, sabemos lo que sucede.

Entonces, lo que puede pasar, si seguimos en esta tesitura, es que nos enfrentemos a una distopía inteligente,

bajo la cual se agudizarán los reemplazos de los trabajadores por máquinas, a efectos de permitir a los empresarios aumentar sus ganancias; se proponen mecanismos “esquizofrénicos” bajo los cuales se regulan aspectos que son convenientes para ciertos sectores y liberales¹⁴, abiertos para otros; se está produciendo una normalización sistemática de derechos fundamentales, con un alto impacto en el sistema político¹⁵.

De esta manera, trae posibles opciones de regulación que hoy se encuentran en discusión en algunos sectores de la academia. Por un lado, considerar la importancia del principio precautorio, bajo el cual, uno de sus efectos resultaría que es posible fomentar el desarrollo tecnológico cuando esté demostrado que no va a causar un daño. Lo peligroso no es la IA, sino la IA no regulada. La IA puede ser muy útil para realizar análisis, para el desarrollo de política criminal, para detectar problemas sistémicos a partir de su lógica de patrones, pero tiene que estar alejada de la toma de decisiones. Es

14 Ejemplo la clásica discusión sobre la no regulación de la tecnología pero sí de la propiedad intelectual en este plano: entonces no regulación, pero sí regulación cuando se afectan determinados intereses.

15 Puso en evidencia los efectos del Brexit cuando está comprobado que hubo una alta intervención de la tecnología (caso Cambridge Analytica)



por este motivo, dice el expositor, que la IA debe estar regulada de modo que sea el medio que se puede utilizar para

analizar, pero nunca la que toma la decisión.



COMITÉ ACADÉMICO

La evaluación y revisión de las comunicaciones del encuentro fueron consideradas por el Comité Académico convocado para el encuentro

Dra. Wilma Arellano Toledo (UNIR). España

Mg. Federico Daniel Arrue (UNS). Argentina

Dra. Rosa Avila Paz de Robledo (UNC – UNLaR). Argentina

Dr. Fernando Barrio (QMUL). Inglaterra

Dr. Alejandro Chamatrópulos (UNT). Argentina

Dr. Mario Gerlero (UNLP – UBA). Argentina

Dr. Sebastián Gomez (PJ NEUQUEN – UNRN). Argentina

Mg. Abog. Corina Iuale (UNS – UNRN). Argentina

Abog. Jose María Lezcano (UNLP). Argentina

Abog. Ernesto Liceda (UNLP). Argentina

Abog. Ismael Lofeudo (UNLP). Argentina

Abog. Noemí Olivera (UNLP). Argentina

Dr. Rolando Joaquín Ortega Hernandez (UNIR). España

Mg. Manuel Martín Pino Estrada (OAB). Brasil

Dr. Diego Robledo (UNC – UNLaR). Argentina

Dr. Ariel Vercelli (CONICET – UNMdP). Argentina



Equipo de recepción de trabajos, gestión y edición:

- Abog. Ignacio Zelasqui
- Est. Martina Gutierrez Iuale
- Abog. Marina Flammini
- Est. Pablo Molina
- Est. Ana Visconti

Redes y Medios:

- Est. Martina Gutierrez Iuale
- Est. Melissa Chao

Web Site:

<http://www.gecsi.unlp.edu.ar/>

<http://derechoytecnologia2020.hol.es/>

Facebook: <https://www.facebook.com/Encuentro-de-Docentes-Investigadores-y-Estudiantes-de-Derecho-y-Tecnolog%C3%ADa-109145367626484/>

Instagram: <https://www.instagram.com/derechoytecnologia2020/>

Twitter : <https://twitter.com/dertecno2020>

YouTube: <https://www.youtube.com/channel/UChO3d8zxHMLPNtiWqS10iuA/videos>

Primera Parte

Presentación: La Inteligencia Artificial Frente al Derecho

Reflexiones sobre la importancia del eje del encuentro y sus discusiones

Prof. Abog. Ernesto Liceda

“Así pues, la perfección y la imperfección son sólo, en realidad, modos de pensar”

Barauch de Espinosa, “Ética demostrada según el orden geométrico”

En el primer eje del encuentro, que tuve el honor de moderar, se discutió profundamente la naturaleza y el uso de la Inteligencia Artificial (en adelante IA) en la sociedad. Los trabajos presentados, que el lector encontrará de sumo interés, versaron sobre diversos temas que fueron desde el nombre mismo dado a la tecnología hasta su uso en el marketing y en los sistemas judiciales sin dejar de lado en ningún momento el análisis de la

posible vulneración de derecho al momento de implementarla.

Pero si bien los trabajos son sumamente interesantes, particularmente entiendo que el desarrollo del debate y las reflexiones que se generaron han sido, por lejos, lo más valioso del encuentro. Por ese motivo a continuación listaré algunas de las preguntas que fueron surgiendo y algunas respuestas o

primeros acercamientos.

¿Existe una disputa entre el humanismo y la tecnología? ¿Es necesaria una regulación sobre la tecnología que incluya, o no, sistemas de auditoría? ¿Los sesgos en la IA son sólo generados por el programador o la IA puede generar sus propios sesgos? ¿Puede utilizarse de la misma manera la IA para el diseño de políticas públicas y para la aplicación a casos particulares? ¿Debemos incluir expresamente el principio pro hómīne en los sistemas regulatorios? ¿Alcanza con la inclusión de parámetros éticos en el desarrollo de la IA? ¿Es necesario un cambio completo en el sistema jurídico, cortar amarras con el derecho decimonónico? ¿Debe utilizarse la IA aún a costa de perjudicar la fuente de trabajo de millones de personas? ¿Les son aplicables a las licencias de uso de los desarrollos tecnológicos los tratados internacionales en derechos humanos? ¿Puede dejarse en manos de la IA el control de expresiones en las redes sociales o la decisión final debe estar siempre en manos de un ser humano? ¿Incluso en un sistema perfecto se pueden vulnerar los derechos de las personas? ¿Puede la utilización de IA en el sistema judicial generar un estancamiento en el orden público

internacional (o incluso en el orden jurídico local)? ¿Podría la IA ser fuente del derecho? Por último, y en este caso no en forma de pregunta puesto que fue prácticamente unánime la opinión de los participantes, la tecnología no es neutral.

Como puede verse la dinámica del encuentro y los conocimientos de los participantes en las diferentes materias dieron por fruto algo mucho más valioso que la suma de las partes.

Es preciso detenernos entre la posible disputa entre el humanismo y la tecnología. Tal vez sería más correcto decir la disputa entre la implementación de tecnologías que avasallen los derechos de la mayoría de las personas y el no uso de dichas tecnologías. Punto que se asoció rápidamente con la cuestión de sí la tecnología vulnera derechos porque es imperfecta o sí, incluso un sistema perfecto, genera los mismos resultados. La mayoría de los participantes coincidieron en que incluso un sistema perfecto puede vulnerar derechos. Pero tal como refiere Espinosa en la cita que abre el presente capítulo, la perfección y la imperfección son sólo modos de pensar, por ello siempre va a depender del punto de vista de cada persona el entendimiento de sí un sistema es o no perfecto. Para algunos un sistema

que resuelva 100 causas penales por segundo con un margen de error de un 1% sería perfecto, puesto que terminaría con el atascamiento en tribunales, para otros que un inocente termine preso por la resolución de un software es inaceptable. Tal vez haya quienes piensen que la IA comete una cantidad similar de errores que el humano por lo que no sería un problema, pero también quienes entiendan que una de las más antiguas luchas de los hombres ha sido ser juzgado por sus pares, por lo que sería un retroceso en la conquista de derechos. Y obviamente habrá quienes entiendan que una máquina es incorruptible mientras otros planteen que la IA va a juzgar en base a las creencias de sus programadores. Esto último nos lleva directamente a dos cuestiones que se trabajaron en el encuentro, las cuestiones relativas a los sesgos además de la forma y necesidad -o no- de incluir a la ética en el desarrollo de la IA.

En lo que a los sesgos refiere el debate resultó sumamente enriquecedor. ¿Los sesgos de la IA son sólo generados por el programador? La respuesta surgida del debate plantea que no. Por una parte es claro que el técnico, al momento de llevar adelante su trabajo puede volcar sobre el sistema algunos sesgos propios sin

intención directa de hacerlo. A modo de ejemplo, una persona socializada en un contexto patriarcal y machista podría, incluso sin intención, desarrollar la IA con algunos sesgos vinculados con axiomas o concepciones disvaliosas para un gran sector de la sociedad actual. Llevándolo a un extremo, al solo efecto de que el ejemplo sea lo más claro posible, el desarrollador en cuestión podría volcar en un sistema de reconocimiento facial algunos sesgos vinculados con el maquillaje o peinado de una mujer y la profesión que ejerce o con el uso de determinada vestimenta y la posibilidad de que cometa un ilícito. Pero la IA también puede generar sus propios sesgos, muchas veces como reflejo de las desigualdades sociales existentes en el lugar donde se implementa. En este sentido se puso como ejemplo un caso de EEUU donde un sistema de IA generaba indicadores sobre la posibilidad o no de que determinada persona cometiera un delito. A causa de la situación socioeconómica de ese lugar el sistema terminó “aprendiendo” que si la persona era de color y estaba dentro de determinado rango etario las posibilidades de que llevara a cabo el ilícito se incrementaban enormemente. Como puede verse este es un punto central al momento de decidir qué poder de

decisión se le va a otorgar al sistema.

Otra cuestión íntimamente ligada a la anterior es la derivada de la inclusión de parámetros éticos al momento de desarrollar IA. Se trata sin duda de un tema ampliamente discutido en, prácticamente, todos los foros especializados en este tema donde la gran mayoría pareciera concordar en que deben ser incluidos. Me permito un pequeño paréntesis, ¿de qué hablamos cuando nos referimos a la ética? ¿Quién sería el que determine cuál parámetro ético aplicar? La ética como disciplina se encarga del estudio de la moral, de la concepción de lo bueno y lo malo, lo justo y lo injusto, etc. mientras que si lo tomamos como atributo de una persona determinada se asocia más al cumplimiento de los mandatos morales de la sociedad donde transcurre su vida. Sin perder de vista la frase que da comienzo al presente capítulo y la muy breve explicación sobre algunas acepciones de la ética me permito preguntar, siendo que cada sociedad, e incluso cada grupo, puede tener su propia visión del mundo y por ende su moral ¿sólo los miembros de una sociedad podrían desarrollar sistemas de IA para dicha sociedad? ¿Será necesaria la generación de un comité de ética que evalúe los sistemas que se

implementaran? ¿Debe dejarse a cada programador o empresa la implementación de la ética según su propia comprensión? ¿Debiera la CIDH (en nuestro caso), la ONU o algún otro organismo transnacional establecer parámetros éticos mínimos para las IA a nivel regional o global? Como se ve las preguntas siguen generando más preguntas.

Es interesante llevar adelante un somero acercamiento a algunas de las distintas soluciones pensadas desde lo jurídico. En algunos casos, particularmente desde el “mercado” y en sintonía con todo lo planteado en lo que a la tecnología refiere, se propone la autorregulación. Esta postura, basada en las ideas de la libertad de contratación y responsabilidad empresaria, entiende que la mejor forma de que la IA se desarrolle en “beneficio de toda la sociedad” es dejar que sean sus creadores y explotadores en conjunto con sus clientes generen el marco normativo de su uso. Es claro que esta tesitura oculta la asimetría clara y diferencias de poder entre las distintas partes y que queda por demás demostrada en todo lo que hace a la protección de la intimidad en internet, por solo citar un ejemplo.

Otra de las posibles soluciones parten desde la regulación en el marco normativo

positivo de cada país. Lo que abre un gran abanico de posibilidades y nuevas preguntas. Continuando con el orden establecido al principio de este capítulo podemos comenzar analizando si es necesaria la inclusión de sistemas de auditorías en una norma reguladora de la IA con el fin de minimizar la generación de sesgos y daños a aquellas personas expuestas a dicho sistema. Imaginemos que la respuesta sea negativa, en ese caso no queda mucho más para pensar. Pero si la respuesta es afirmativa podremos avanzar en cuestiones sumamente interesantes. Por un lado sí la norma debe aplicarse a cualquier sistema de IA o sólo a aquellos que tengan un piso mínimo de impacto social, no es lo mismo un sistema de reconocimiento facial callejero que el análisis de cumplimiento de metas en una empresa. Por otro lado, la auditoría ¿tendría que ser aplicada por terceros, por un organismo oficial o se tendría que generar un modelo en conjunto entre el sector público y el privado? Por último (sólo a los efectos del presente capítulo) ¿la auditoría tendría que ser automática o con intervención humana?

En lo que respecta al impacto en la economía social, más estrictamente en lo que hace al trabajo de los humanos, es

menester detenernos a analizar algunos puntos clave. Hace un tiempo, ante la pregunta –afirmación sería mejor decir- de que a causa de las innovaciones tecnológicas estamos atravesando cambios sin precedentes en la historia de la humanidad, me limité a decir que la historia de la humanidad está atravesada por cambios sin precedentes y eso, de por sí, constituye más una constante que nos da herramientas para afrontar la presente situación. Por demás está decir que resulta obvio que el siglo XIX a pocos se le podría haber ocurrido la IA o la impresora 3 o 4 D, pero lo cierto es que la revolución industrial del siglo anterior y la total instalación de la máquinas en el proceso productivo generó cambios que tal vez nos permita un atisbo de lo que podemos esperar en la actualidad. En este sentido sería esperable un importante cambio en el modelo productivo que dejaría fuera de dicho sistema a una gran masa de trabajadores que tendrían que reconvertirse para poder ser parte de la fuerza laboral nuevamente. Siendo esto bastante claro resulta poco comprensible porqué esperar a que suceda para tomar las medidas necesarias para que ello no ocurra, en otras palabras, porqué esperar los efectos para tomar medidas sobre las causas. Tranquilamente se podría ir trabajando

sobre la reconversión del sistema laboral (menos horas de trabajo, capacitación, retraso en la implementación de la tecnología, cambios en los modos de consumo, etc.) para luego incorporar la tecnología en sí. Poco sentido le veo a permitir un mayor enriquecimiento de sectores ya concentrados a costo de la pauperización de colectivos que ya sufren una situación para nada acomodada.

La disputa aparece siempre entre la tecnología y la persona, entre la máquina y el humano pero debemos tener presente que ello es una falsa disyuntiva. La lucha es siempre entre humanos, entre aquellos que se benefician de un determinado sistema (o cambio del mismo) y entre los que lo padecen. En la sociedad red el rol que debe cumplir el Estado se encuentra en permanente tensión por diversos factores, entre ellos la pérdida de soberanía territorial, la existencia de grupos económicos que cuentan no sólo con mayor poder económico sino también con mayor información sobre la población que habita en dicho territorio, ONGs internacionales que dicen representar a determinados colectivos mientras son financiadas por entidades privadas que persiguen objetivos diversos, movimientos sociales transnacionales, grandes monopolios u oligopolios productores y

distribuidores de información por múltiples canales y un enorme etc. En ese contexto de disputas sobre el sentido del Estado, éste último sigue siendo, al menos por ahora, el único actor que puede poner algún tipo de freno o establecer algunas formas de mitigar los daños derivados de la implementación amoral de la tecnología. Entonces ante la pregunta sobre si les son aplicables a las licencias de uso de los desarrollos tecnológicos los tratados internacionales en derechos humanos, la primera respuesta podría ser un no. Puesto que, según la teoría predominante, dichos tratados son dirigidos al Estado. Pero hay que tener en cuenta que los Estados no se obligan meramente a no violar los derechos humanos sino a permitir que los mismos no sean violentados por terceros. Entonces, si bien no los tratados existentes no se les aplicarían directamente los Estados están obligados a dictar normas tendientes a la protección de las personas expuestas al uso de dichas tecnologías. Tarea nada sencilla teniendo en cuenta la situación actual a la que se hacía referencia anteriormente. Demás está decir que dicha situación puede cambiar rápidamente de la mano de acciones tales como la aparición de impuestos globales a multinacionales y de la voluntad de organismos multilaterales y

de los llamados países centrales de tomar cartas en el asunto.

Ante todo lo planteado hasta ahora surge de cierto el que, tal vez, sea el eje central de la discusión. La continuidad o no del sistema jurídico decimonónico. Evidentemente la respuesta no es simple y esbozar una solución completa escapa al espíritu del presente capítulo es posible dar algunas líneas o pautas para problematizar la cuestión.

Un tema que viene siendo muy debatido desde hace ya un tiempo es el de la responsabilidad por los hechos de la IA, sea la misma penal o civil. Hay quienes plantean que la responsabilidad siempre será del dueño o titular del sistema, otros agregar a aquel o aquellos que se benefician de su usufructo tomando, en algunos casos, como base las teorías que versan sobre la cosa riesgosa. Otros piensan que lo ideal sería reconocerles a las IA (robots, etc.) personalidad jurídica y que respondan por las acciones no pensadas por sus diseñadores. Algunos de los que plantean esta solución esgrimen como ejemplo algunos fallos donde se reconoció como persona jurídica no humana a algunos animales (claro está que en ese caso fue para reconocerles algunos derechos y no para hacerlos responsables de sus acciones).

La primera postura es criticada, entre otros, con planteos utilitaristas, sí se quiere, que parten de que al hacer responsables a los diseñadores y otros sujetos de las acciones cometidas por la IA, que no pudieron ser previstas en forma alguna, implicaría un freno a la evolución e implementación de una tecnología que vendría a “beneficiar a toda la sociedad”. También se critica el hecho de responsabilizar a una persona, física o jurídica, por hechos que escapan de su capacidad de control y previsión sería incompatible con el principio de justicia (sobre este punto en particular se habla de la responsabilidad sobre las cosas riesgosas).

Las críticas a la segunda postura parten desde distintas perspectivas. Por un lado porque al convertir a la IA en un ente responsable se quita toda responsabilidad sobre sus diseñadores y sobre aquellos que usufructúan el sistema. Por el otro porque no sería del todo claro con que patrimonio respondería frente a los daños ni tampoco que tipos de sanciones podrían disuadir a una IA para que no lleve a cabo una determinada acción. Una de las posibilidades que se proponen es, a imagen y semejanza de algunas personas jurídicas, brindar a las IA con un patrimonio de partida, claro es que la

discusión sobre el monto y sostenimiento de ese patrimonio difícilmente sean simples.

Como puede verse ambas soluciones parten desde la concepción actual del derecho, buscando asimilar estas nuevas situaciones a lo ya conocido sin detenerse a pensar en formas de resolución desde distintas perspectivas.

Para poder empezar a pensar soluciones alternativas es preciso detenernos a pensar en el fondo de las cuestiones y no en cada hecho concreto. La idea de que el derecho positivo puede regular cada aspecto de la vida en sociedad fue incumplible desde su nacimiento pero tal vez se acercó bastante a su objetivo en algunos momentos históricos, la etapa que nos toca no sólo no es uno de ellos sino que se aleja cada vez más de la utopía codificadora. Por ello resulta imprescindible salir del micro derecho y pasar al macro, en otras palabras dejar de intentar regular todas las situaciones y pasar a (re) establecer principios rectores compatibles con la sociedad actual. Sólo por citar un ejemplo, es claro que si hay un concepto esencial en la sociedad de la información (o sociedad red) es el de la información pero no se cuenta con un acuerdo claro de los distintos sectores de que se va a entender legalmente por

información y que categorías pueden conformarlas. Hay una primera categoría establecida en la ley 25.326 (protección de datos) pero que no se ha integrado correctamente con el resto del sistema jurídico y que sólo refiere a ciertos tipos de informaciones, otro acercamiento al tema se dio a través de la llamada “ley de medios”, y pueden encontrarse otras acepciones en distintas normas (código civil, ley de inteligencia, etc.) pero no un concepto integrado que de densidad a dicho concepto. De hecho el código penal tiene figuras delictivas que refieren a bases de datos o a datos pero sin definirlos en forma alguna, ante lo cual es preciso “rellenar” el concepto con la ley de protección de datos, aunque dicha interpretación no necesariamente es obligatoria para el juez que deba resolver una determinada situación.

Otro punto a tener muy en cuenta es el que se vincula con la mal llamada “identidad digital”, siendo que en nuestro marco normativo no existe una definición clara de identidad a secas es realmente complicado pensar en resolver los problemas derivados de la “digital”. Una vez resuelto que se entiende por identidad, podremos avanzar sobre cuestiones relativas a la diferenciación entre identidad e identificación y cuál

concepto corresponde a cada situación y en qué casos. Pero ello no puede ser resuelto agregando 500 nuevos artículos a los diferentes códigos que forzosamente quedarán desactualizados en muy poco tiempo, sino de acuerdos macro que permitan establecer principios claros donde los llamados a resolver los conflictos puedan hacer pie para llevar a

cabo su tarea. Tal vez sea el momento de parar el carro unos momentos, pensar prospectivamente y definir de cierto cuáles son los valores que queremos que el derecho tutele en la sociedad en la que vivimos. Tal vez sea el momento del derecho centrado en principios y no en normas positivas.

Capítulo 1

Planteos generales en el uso de la Inteligencia Artificial

INTELIGENCIA ARTIFICIAL: UNA DEFINICIÓN ENGAÑOSA¹⁶

Roberto Nelson Bugallo¹⁷

RESUMEN:

Se adjudica a Sun Tzu en “El arte de la guerra” mencionar que lo que es familiar no provoca ni llama la atención. Y algo tan cotidiano como el lenguaje no despierta suspicacias aunque se aplique a las tecnologías digitales conceptos como el de inteligencia artificial adjudicando una relación que toma como modelo la inteligencia humana.

Esta conformación antropomórfica modelada sobre los procesos de la mente humana busca transponer conocimientos de la biología neuronal - como los derivados de la sinapsis- a un universo cibernético, pero entrando por la puerta amable del lenguaje cotidiano, aunque las similitudes sean bien escasas o inexistentes.

La pretensión de crear sistemas que piensen como humanos a través de redes neuronales artificiales y sobre todo que actúen como agentes inteligentes deslegitimando las decisiones de la propia conciencia nos enfrenta a un dilema en el que el lenguaje opera como una herramienta formidable para naturalizar prácticas dominantes.

Palabras claves: inteligencia artificial, antropomorfismo digital, lenguaje simbólico, falacias de asimilación, tecno-ideología.

16 Enlace al video: <https://youtu.be/Y5yOGwHRFHA>

17 Docente investigador, Fac. de Cs. Jur. y Soc., UNLP; Fac. de Derecho, UBA; Fac. de Cs. Sociales, UNCPBA. Abogado, Integrante del GECSI -Grupo de Estudio de la Complejidad en la Sociedad de la Información- mail: robertobugallo@jursoc.unlp.edu.ar

...Y EL HOMBRE CREÓ A LOS DIOSES A SU IMAGEN Y SEMEJANZA...

Señalan los estudiosos de la antropología que el paso del hombre cazador-recolector al hombre cultivador, no solo representó un cambio en las conformaciones sociales comunitarias, sino también –y muy especialmente- un cambio en la mirada del mundo circundante. El cazador-recolector, fundamentalmente nómada, iba detrás de las manadas de animales que consistían sus presas y de los frutos o semillas que se producían en diversos lugares y de acuerdo a las estaciones. Los pequeños grupos eran parte de un paisaje que mutaba según se trasladaran. El paso a la agricultura, no solo permitió que pudieran establecerse en un territorio, e incrementó la población, sino que cambió su mirada de ubicación con el entorno. Ya no es más otro animal vagabundo, ahora es quien se instala en un lugar al que convierte en “su” lugar y adquiere una mirada antropocéntrica de su hábitat. El hombre ya instalado en una comarca se siente el señor, el centro, el decididor.

Pero casi en simultáneo, toma conciencia de sus limitaciones, de su mortalidad, de que solamente puede estar al mismo tiempo en

un único sitio, y apenas conocer a los semejantes en lo que es su entorno. Y entonces crea a los dioses y los hace a su propia imagen, los dota de sus sentimientos humanos, pero les agrega además todo aquello de lo que carece y envidia: la inmortalidad, la omnipresencia, la facultad de conocer los pensamientos y las acciones más recónditas, el poder y la sabiduría para predecir lo que vendrá....y así será durante varios miles de años, en los que los dioses, se transforman, se reciclan o adquieren nuevas visibilidades, nuevas definiciones, u otros nombres, pero conservando siempre esas extraordinarias facultades que los diferencian de los simples humanos

LA IRRUPCIÓN DE LAS TECNOLOGÍAS DIGITALES

Las dos últimas décadas produjeron un cambio contundente y dramático en casi todo lo relacionado con nuestra existencia, sea en lo social, lo político o lo económico, en lo individual o lo colectivo. Cambiamos la forma de relacionarnos, de comunicarnos, de informarnos y de tomar decisiones. Las tecnologías digitales modificaron los valores y conceptos cuya construcción colectiva se cimentó en largos espacios de tiempo e involucró a varias generaciones.

Implicaron a las relaciones sociales y a los procesos de producción de la subjetividad y modificaron casi todos los segmentos de la vida privada y pública alterando los límites de la intimidad y la privacidad, la forma en que nos construimos como personas y los procesos relacionales entre semejantes. Ni hablar del impacto que están produciendo en lo político, donde desmontan, entre otros, la noción del Estado que habíamos reconocido en los últimos siglos, al igual que los conceptos del poder o la hegemonía.

Y todo esto se produce en un espacio de tiempo asombrosamente escaso, aún para quienes están acostumbrados a la vertiginosidad de la época actual.

Pero quizás lo más notable de la que algunos llaman la era del antropomorfismo digital es que estos cambios revolucionarios se producen sin una revolución (al menos con el alcance tradicional del concepto) sino a través de una incorporación naturalizada.

LA APROPIACIÓN DEL LENGUAJE

“Algo que es familiar no despierta la atención”. Se adjudica esta frase a Sun Tzu en el “Arte de la guerra” Y pocas cosas nos son tan usuales como el lenguaje. Las tecnologías digitales han encontrado la puerta amable para integrarse a nuestras vidas sin despertar suspicacias ni

resistencias. Pero el lenguaje no es (y nunca lo ha sido) neutro o inofensivo. Los lenguajes -todos- no solo arrastran una fuerte carga ideológica, sino que su utilización política ha servido como ingreso de muchas colonizaciones culturales (recuérdese el vaciamiento de la lengua de los guaraníes quienes conservaron el idioma pero con los contenidos culturales de los conquistadores españoles)

Las tecnologías digitales han cambiado rápidamente de estatuto. Lo que en sus inicios fue un proceso para permitir el archivo y manejo más sencillo de la información ha devenido en un aumento del control más masivo e imperceptible resultando cada vez menos destinado a brindar información como a digitar las conductas de las personas

Crecientemente se fía menos de los saberes o reflexiones de los humanos y se deriva a las elecciones de los algoritmos, Puede argüirse que las tecnologías procesan millones de datos y que pueden llegar con mayor facilidad a las conclusiones correctas haciendo cada vez más superflua la intervención humana. Pero lo que se estima correcto no siempre es sinónimo de mejor o más recomendable, ni siquiera de verdad o verdadero.

Hay una construcción de la verdad que se reviste de la *auctoritas* que prescinde del

elemento humano y que al no poder apelar a la capacidad moral de las tecnologías digitales captura los términos del lenguaje conocido, pero vaciándolo de contenido.

LA INTELIGENCIA ARTIFICIAL

Para limitar o neutralizar las resistencias se toman como modelo expresiones del mismo campo semántico, de contenido antropomórfico, pero atribuyéndoles a las tecnologías digitales cualidades humanas. Y la inteligencia de los humanos es precisamente el poder de evaluar situaciones y extraer conclusiones.

El modelo es entonces nuestro cerebro al que adjudicamos una arquitectura sistémica conformada por redes neuronales que liberan neurotransmisores para llevar y traer información.

Nuestra capacidad evolutiva cimentada en el desarrollo cerebral y manifestada en la “*inteligencia humana*” conlleva una carga de prestigio simbólico irresistible para trasladarla al término “*inteligencia artificial*”. Y todo eso sin salir del lenguaje cotidiano.

Hoy la variable tecnológica construye un léxico completo que incluye términos como redes neuronales artificiales, chips sinápticos, o algoritmos genéticos en un forzado proceso de transmutar las ciencias

cognitivas para asignarles a los sistemas digitales una estructura supuestamente similar al cerebro humano.

La empresa Intel, fabricó un chip al que denominó “*neuromórfico*” con capacidad para aprender gracias a los millones de “neuronas” y los millones de “sinapsis”. Pronto nuestros sistemas digitales podrán incorporar un “*procesador neuronal*” y este neoléxico se muestra como la expresión más visible de la conexidad en una relación que pretende mostrarse como simbiótica

Ya con la tranquilidad de contar con una “*inteligencia artificial*” engañosamente asimilada a la inteligencia humana está abierta la era digital antropomórfica. Permite marginar sin pudor a quienes objetan esta nueva etapa como seres “*no inteligentes*” o peor, como herejes iconoclastas que no quieren reconocer las virtudes omnipresentes, inmortales, predictivas y hegemónicas de los nuevos dioses digitales.

Franqueada la puerta de ingreso, nos vamos deslizado suavemente a una “omnisciente” hiperconectividad a través del “internet de las cosas”, a las ciudades “inteligentes” (smart cities), a las plataformas de streaming service, a los digital assistants, cuya misión pareciera consistir únicamente en facilitarnos la vida y proveernos de todo lo que necesitamos.

Porque la realidad es que los necesitamos. Primero se comenzó por recoger los miles de millones de datos que diariamente brindamos al coleccionar información, buscar páginas, mirar videos, comunicarnos entre si. ¿qué es lo que vemos?, ¿durante cuánto tiempo?, ¿que compramos?, ¿con quién hablamos?, etc, todo queda almacenado y registrado. Nuestros celulares, tablets, computadoras, y cuanto artefacto usamos para ingresar a las redes, páginas, blogs etc, dejan permanentemente rastros informáticos que son reunidos y analizados por las grandes corporaciones proveedoras de servicios digitales. En los dos últimos decenios el alcance totalizador de estas tecnologías no cesó de introducirse en todos los segmentos de nuestra vida.

El siguiente paso fue orientar la acción humana y ahora son estas tecnologías digitales las que están decidiendo quienes serán seleccionados para cubrir cargos laborales o cómo se van a formular los diagnósticos médicos o a diseñar casas inteligentes para que vivan las personas inteligentes que son las que consumen los productos y dispositivos que ofrece la Inteligencia Artificial

Porque la tecnología no es neutra –quizás nunca lo fue- pero hoy se ha consagrado como *tecno-ideología*, en función de un

modelo que ha mutado de configurar inicialmente sistemas acumulativos de datos para permitir el tráfico veloz de información a ser entidades que dictaminan la verdad a partir de la interpretación digital de situaciones.

LA FALACIA DE LA ASIMILACIÓN

El término de “inteligencia artificial” llegó en 1956 de la mano de un informático con conocimientos bastante elementales de neurociencia para designar con esa palabra la ingeniería de “hacer máquinas inteligentes”, pero recién en la última década del siglo 20 se generalizó.

En verdad, sostener la existencia de una inteligencia basada en lo digital y modelada sobre la inteligencia humana es equivocado por varias razones. Estas estructuras son solo la representación de sistemas complejos que son alimentados por algoritmos y cuya tarea es el tratamiento de flujos de información abstractos. Aún conectados a estructuras similares su función quedaría reducida a traducir elementos del mundo real a códigos binarios descartando una serie infinita de dimensiones que el cerebro humano puede captar y que escapan a un modelo matemático. Esta traspolación es la versión limitada y cercenada de lo que entendemos como inteligencia humana inescindible de

su relación con el entorno sensorial, afectivo, emotivo y un largo etcétera en el que nos movemos. No es posible concebir ninguna inteligencia que subsista solo recluida en sus propias lógicas.

La inteligencia humana no puede dissociarse de un contexto indeterminado y permanentemente abierto muta constantemente. No es solamente la capacidad de adaptabilidad al estilo de la evolución darwiniana, sino la capacidad de modificarse constantemente, repensarse continuamente para volver a cuestionarse frente a lo no esperado y reinventarse en un proceso sin fin.

Son estas algunas de las razones que tornan utópica cualquier asimilación entre la inteligencia humana y la llamada inteligencia artificial porque esta última está estructurada sobre bases funcionalistas y solo para responder a los fines para los que fue creada.

Sin embargo, el incremento exponencial de la capacidad de generación y propagación del discurso digital, debido al despliegue de internet, se ha dado en forma paralela a la sofisticación de los mecanismos de control facilitados por las tecnologías cada vez más vigilantes y totalizadoras.

No escapa a la elaboración de este trabajo

que hoy ya son muchos los cuestionamientos que surgen de distintos sectores sobre las tecnologías digitales, la apropiación de los datos, la utilización de las redes y la segmentación del conocimiento y que mayormente se apela a la falacia de la neutralidad técnica cuando se está convirtiendo en el negocio manipulado mas fabuloso de todos los tiempos. Tampoco ignoro el impacto de un video reciente que desnuda su utilización a escala planetaria ayudado por la naturalización con que estamos aceptando estas prácticas.

Apenas he ensayado escarbar en un nicho tan presuntamente inocente como es el uso trastocado de los términos que hoy hace que hablemos de la inteligencia artificial como un sucedáneo de la inteligencia humana, soslayando el tramposo abuso del lenguaje que vuelve a erigirse como elemento de dominación cultural banalizando su penetración y debilitando las alertas que operan naturalmente.

En aras del impulso de “necesitar” de los bienes comunes que proporcionan las tecnologías digitales, una parte importante de esta generación ha resignado nuestros modos de ser en común, relegando un humanismo en el que la pluralidad y el respeto por la misma constituyen un principio inalienable. Solo si dejamos de lado la

fascinación y recuperamos la mirada crítica tendremos una oportunidad de que estos nuevos dioses tecnológicos no vuelvan a emular a Saturno y terminen devorándonos.

BIBLIOGRAFÍA

“*El lenguaje como instrumento de la dominación totalitaria en H. Arendt*” Bermúdez Reina, Christian. Ponencia. Universidad Libre de Colombia. 2016

“*La humanidad aumentada*” Eric Sadin, Ed. Caja Negra, 2017

“*La inteligencia artificial o el desafío del siglo*”, Eric Sadin, Ed. Caja Negra, 2020

“*La jaula del confort*” Esteban Magnani, Autoría Editorial, 2019

“*La locura del solucionismo tecnológico*” Evgeny Morozov, Capital Intelectual, 2016

“*Digitalizados. La vida humana en un mundo algorítmico*”, Facultad de Artes, UNLP, Revista, agosto 2018

“*El arte de la guerra*” Sun Tzú, <https://freeditorial.com/es/books/el-arte-de-la-guerra/related-books>

“*¿Por qué el capitalismo puede soñar y nosotros no?*” Alejandro Galliano, Siglo XXI, 2020.

LIBERTAD DE EXPRESIÓN E INTELIGENCIA ARTIFICIAL EN LA RED¹⁸

Manuel Larrondo¹⁹

Nicolás Mario Grandi²⁰

RESUMEN:

La IA es utilizada para una amplia gama de acciones, desde detectar aquellas infracciones de copyright hasta seleccionar y remover contenido vulneratorio de los “términos y condiciones” de las plataformas.

Es evidente que tal proceder repercute en el ejercicio del derecho humano a recibir, investigar y difundir información.

Una primera aproximación al empleo de IA de parte de las plataformas podría considerarse adecuado para la remoción de contenido violento o que incita al odio.

Sin embargo, sin moderación humana que contextualice y traduzca adecuadamente la expresión, puede existir un serio riesgo de que la arbitrariedad prevalezca.

Por lo tanto, en este trabajo planteamos que el desafío algorítmico-jurídico consiste en lograr armonizar la convivencia entre el empleo de la IA para moderar contenido en línea y los estándares internacionales de libertad de expresión mediante la revisión y/o supervisión de un ser humano de toda

18 Enlace al video: https://youtu.be/vy1QSwm_s2c

19 Docente e investigador. Facultad de Periodismo y Comunicación Social UNLP. Mail: larrondomanuel@gmail.com

20 Abogado, Docente e investigador. Facultad de Periodismo y Comunicación Social UNLP. Mail: drgrandinicolos@hotmail.com

decisión automatizada que impida o remueva contenido en línea que, en particular, se relacione con temas de interés público.

Palabras clave: Moderación - contenido- Internet - intermediarios -redes sociales -

INTRODUCCIÓN

La libertad de pensamiento y expresión humana es la base fundamental de toda sociedad democrática.

Así lo reconocen el art. 19 de la Declaración Universal de DDHH al igual que el art 18 (libertad de pensamiento) y art 19, 1) y 2) del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) al prever que “nadie podrá ser molestado a causa de sus opiniones” así como también que toda persona gozará del derecho a “buscar, recibir y difundir informaciones e ideas de toda índole” sin consideración de fronteras o “procedimiento” que elija.

Sin embargo, al mismo tiempo reconoce que ese derecho puede estar sujeto a restricciones que deben ser fijadas por ley necesaria para: a) asegurar el respeto a los derechos o a la reputación de los demás y b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

Por su parte, el Sistema Interamericano

de Derechos Humanos consagra en igual sentido y alcance de protección amplia a ese derecho en el artículo 13 de la Convención Americana de DDHH (CADH), con la particularidad de que expresamente prohíbe la censura bajo cualquier modalidad y sólo la contempla en forma previa para proteger a los derechos de la niñez y adolescencia. En igual sentido, destaca que quien ejerza este derecho se encuentra sujeto a las responsabilidades ulteriores que deben estar fijadas por ley respetando su necesidad, legitimidad y proporcionalidad.

Respecto a las posibles restricciones y responsabilidades posteriores al ejercicio del derecho, advertimos que el Comité de DDHH de la ONU -interpretando los alcances del art 19 del PIDCP- se inclina por una postura aún más protectora al considerar que la libertad de opinión “no autoriza excepción ni restricción alguna” a su ejercicio, ya sea “por ley u otro poder” (ONU, 2011).

Es evidente que los límites y alcances del

ejercicio de este derecho han sido y son centro de análisis e interpretación complementaria de parte de los principales Organismos internacionales.

Sin ir más lejos, basta con citar la vigencia de la OC 5/85 dictada por la Corte Interamericana que señala que la libertad de expresión no se agota en su faz individual sino que comprende además a la dimensión colectiva de su ejercicio a través de cualquier medio apropiado para difundir el pensamiento al mayor número de destinatarios.

En nuestro país, la Corte Suprema de Justicia de la Nación ha seguido la misma sintonía remarcando en innumerables ocasiones que la libertad de expresión, en su faz colectiva, tiene por objeto proteger el debate público, con amplias oportunidades de expresión de los distintos sectores representativos de la sociedad en la que todos puedan, en un plano de igualdad, expresar sus opiniones y en la que no pueden admitirse voces predominantes (CSJN, 2013).

Estos estándares intercontinentales protectores de la libre expresión fueron consensuados a lo largo de casi todo el siglo XX y principios del presente siglo XXI. Con la irrupción de las redes sociales y demás intermediarios en línea, en la actualidad prácticamente la mitad de la

población mundial ejerce la triple acción de difundir, investigar y difundir información a través de Internet y, en particular, por medio de las principales plataformas que emplean “Inteligencia artificial” (IA) con las que interactuamos día a día.

¿Qué es la IA? De momento no se ha logrado consensuar una única definición a nivel mundial. En esta ocasión nos inclinaremos por citar aquella que brinda la Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de la ONU al decir que es una “constelación” de procesos y tecnologías que permiten que las computadoras complementen o reemplacen tareas específicas que de otro modo serían ejecutadas por seres humanos, como tomar decisiones y resolver problemas (ONU, 2018).

Agrega la Relatoría que en la base de la IA están los “algoritmos” que son códigos informáticos diseñados y escritos por seres humanos que ejecutan instrucciones para traducir datos en conclusiones, información o productos. Así, el enorme volumen de datos de la vida moderna y la capacidad de analizarlos impulsan al desarrollo de la IA. Basta como muestra advertir que el volumen de generación de datos en línea

crece exponencialmente cada segundo a punto tal que en solo un minuto de navegación en Internet “3,5 millones de personas buscan en Google; 900 mil se conectan a Facebook –envían 31,25 millones de mensajes y ven 2,77 millones de videos–, 452 mil tuitean, 46.200 suben fotos a Instagram; se reproducen 4,1 millones de horas de video en Youtube y 70 mil de Netflix. Se trata de un caudal de información que –caracterizado por su volumen, velocidad y variedad– ocasiona un fenómeno muy de esta era, la big data: nueva ciencia de datos masivos, producto de la interacción de dispositivos interconectados electrónicamente. Pasamos de medir la capacidad de almacenamiento de información –o de memorias, para guardarlos–, del inicial kilobyte (mil bytes) al mega (millón), giga, tera, peta, exa, zetta, yotta y ahora se habla de hella (número de 27 cifras) bytes: cada segundo se crean 1,7 megabytes de nueva información” (Daus, 2019).

Este inmenso caudal de datos que generamos a través de las redes sociales, conforman un excéntrico lugar virtual en el que confluyamos con otros humanos al igual que también con “bots” y demás sistemas automatizados basados en IA.

Si bien estos últimos coadyuvan al ejercicio de la libre expresión, al mismo

tiempo han surgido evidencias concretas que nos alertan sobre el serio riesgo de que poco a poco la IA “*usurpe*” el derecho humano a recibir, investigar y difundir contenido en línea al moderar de forma automatizada qué contenido perdura y cual es removido según sus “términos y condiciones”.

IA Y LA MODERACIÓN DE CONTENIDO

Las IA actúa dentro de las principales plataformas reseñadas como un sistema algorítmico de recomendación y clasificación del contenido digital al que los usuarios acceden y comparten. Algunos estudios muestran cómo los sistemas que están optimizados para la participación del usuario pueden tener el efecto de amplificar y priorizar el contenido controvertido que puede distorsionar así al discurso público y amplificar las divisiones sociales (Singh, 2019).

La Relatoría para la libertad de expresión de la ONU ha remarcado que la IA, en el campo de la moderación de contenido, tiene sus aristas positivas, pero también negativas.

Entre los beneficios de su uso, la Relatoría remarcó que la selección

personalizada de contenido aumenta la experiencia en línea de cada persona permitiendo encontrar rápidamente la información solicitada en diversos idiomas. Pero a esa virtud se le contrapone la minimización de la exposición a puntos de vista diversos, lo que interfiere con la iniciativa individual de buscar e intercambiar ideas y opiniones entre grupos ideológicos, políticos o sociales. Esa personalización puede reforzar los sesgos e incentivar la promoción y recomendación de contenido incendiario o desinformación para mantener la participación en línea del usuario (ONU, 2018, párrafo 3).

Esta moderación de contenido, que genera una burbuja informativa, ha despertado el interés de la Unión Europea que alertó que los seres humanos que interactúan con los sistemas de IA deben ser capaces de mantener una autodeterminación plena y efectiva sobre sí mismos y ser capaces de participar en el proceso democrático. Los sistemas de IA no deben subordinar, coaccionar, engañar, manipular, condicionar o agrupar injustificadamente a los seres humanos.

En lo que refiere puntualmente a la red social Facebook, Sandra Alvaro explica que “cuenta con un algoritmo denominado Edgerank que analiza los datos recopilados acerca de nuestros intereses

–los «me gusta» que pulsamos–, el número de amigos que tenemos en común con el emisor de la historia, así como los comentarios realizados, para determinar qué post mostrar en nuestro «news feed» y ocultar las historias «aburridas» (Alvaro, 2014).

Un caso reciente de moderación automatizada de contenido periodístico es el que tuvo como protagonista a la red social Twitter que impidió que los usuarios compartieran un artículo del “*New York Post*” vinculado al candidato presidencial Joe Biden y sus eventuales contactos con un empresario ucraniano. ¿Por qué lo impidió? Porque podría ser contenido dañoso (Cox, 2020).

A MODO DE CIERRE ABIERTO

Ante el excesivo caudal de datos e información, en coincidencia con la Comisión Europea creemos que debe postularse que, en lo que respecta a garantizar el libre ejercicio de recibir, investigar y difundir información, el empleo de IA en las plataformas en línea debe seguir los principios de diseño centrados en el ser humano y dejar una oportunidad significativa para la elección humana (European Commission, 2019).

Si bien la IA en los últimos tiempos ha

mejorado exponencialmente el Procesamiento del Lenguaje Natural (PLN), aún no han logrado entender la totalidad de los matices lingüísticos y culturales por los cuales se expresan los humanos.

Estos problemas también los advirtió el Comité de DDHH de la ONU en tanto a que los algoritmos, a diferencia de los seres humanos, no son hoy capaces de evaluar el contexto cultural, detectar la ironía o hacer el análisis crítico necesario para detectar con exactitud, por ejemplo, el contenido “extremista” o el discurso de odio, sensibilidades culturales, lingüísticos o de género, o el interés público en el contenido. Por lo tanto, tienden más a bloquear y restringir el contenido y así a menoscabar los derechos de los usuarios a ser escuchados y el derecho a obtener información sin restricción ni censura (ONU 2018, párrafos 29 y 37).

Concluimos por ahora en anticipar que el desafío algorítmico-jurídico consiste en lograr armonizar la convivencia entre el empleo de la IA para moderar contenido en línea pero haciéndolo con perspectiva humana, esto es, respetando los estándares internacionales de libertad de expresión y garantizando la revisión y/o supervisión de un ser humano de toda decisión automatizada que impida o remueva contenido en línea que, en

particular, se relacione con temas de interés público.

BIBLIOGRAFÍA:

- Alvaro, Sandra (2014) “El poder de los algoritmos: cómo el software formatea la cultura”, Recuperado el 5/5/18 de <http://lab.cccb.org/es/el-poder-de-los-algoritmos-como-el-software-formatea-la-cultura/> _
- Cox, Joseph (2020) “Twitter Says It Blocked NY Post Hunter Biden Article Because It Contains Hacked Data”. Recuperado el 10/12/20 de https://www.vice.com/en/article/pky7nb/twitter-blocks-hunter-biden-new-york-post?utm_content=1602705151&utm_medium=social&utm_source=VICE_twitter
- Corte Suprema de Justicia de la Nación (2013) “Grupo Clarín S.A. y otros c/ Poder Ejecutivo Nacional y otro s/ Acción meramente declarativa”. Ver voto de la mayoría de Jueces en sentencia del 29/10/2013. Recuperada el 10/12/20 de <https://www.cij.gov.ar/nota-12394-La-Corte-Suprema-declar--la-constitucionalidad-de-la-Ley-de-Medios.html>

- Daus, Gisela (2019) “Walter Sosa Escudero y la big data: el experto ante el diluvio de datos.” Acceso en octubre 2019 ver en:

https://www.clarin.com/revista-enie/ideas/walter-sosa-escudero-big-data-experto-diluvio-datos_0_e9JEpX9e.htm

Walter Sosa Escudero es docente y econometrista. Autor de “Breve manual para conocer la ciencia de datos que ya invadió nuestras vidas” (Ed. Siglo XXI).

- European Commission (2019), “Ethics Guidelines for Trustworthy AI”, B-1049 Brussels .

- ONU (2011) Observación general núm.

34 sobre la libertad de opinión y de expresión, párr. 9; disponible en <https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>

- ONU (2018) “Promoción y protección del derecho a la libertad de opinión y expresión” 29 de agosto de 2018. A/73/348* <https://undocs.org/es/A/73/348>

- Singh, Spandana (2020) “Rising Through the Ranks - How Algorithms Rank and Curate Content in Search Results and on NewsFeeds,” Spandana Singh. Recuperado el 10/12/20 de <https://www.newamerica.org/oti/reports/rising-through-ranks/>

CIBERTOTALITARISMO

UN EXAMEN DE LA IDEOLOGÍA “WOKE/ CANCEL CULTURE” COMO NUEVO PARÁMETRO DE PRÁCTICAS EN EL CAMPO JURÍDICO²¹

Mario S. Gerlero²²

RESUMEN:

La Sociología Jurídica tiene una notable ventaja en el campo jurídico debido al hecho de contar con instrumentos de análisis que permiten develar las estructuras más profundas enterradas de los “diversos mundos sociales” y que constituyen el universo social actual sus causas, desarrollos y consecuencias.

Aquí se trata de recurrir a esta disciplina con el objeto de asir instrumentos para visibilizar mecanismos sociales, culturales y jurídicos que limitan el debate en una democracia plural y compleja, situaciones que obstaculizan la construcción de un consenso comunitario imprescindible en un momento de notables tensiones sociales.

Uno de los hechos sociales que limitan el debate plural es un fenómeno social problemático: “la cultura de la cancelación” que pone en crisis las Instituciones Jurídicas y la racionalidad de la actividad de los operadores del derecho en el campo jurídico. Esto es: en el contexto de la cultura digital del paso en el uso de las redes sociales para visibilizar problemas socio-culturales periféricos a una etapa de negación de la diversidad; situación esta que implica el desplazamiento del activismo, la participación y el compromiso de la sociedad civil (woke) a un nuevo momento en esta secuencia donde la Inteligencia Artificial pasa a ser un recursos para el activismo político radicalizado que podría generar situaciones relacionadas con el “cibertotalitarismo” limitando o anulando la oposición, el

21 Enlace la video: https://www.youtube.com/watch?v=bNw_RAc0fyU

22 Doctor en Ciencias Jurídicas. Docente-Investigador. UNLP; UBA; FONCyT-CONICET; Director del GECSI-UNLP mario_gerlero@yahoo.com.ar

debate y la valía de la sociedad civil.

Palabras claves: Redes Sociales; Cultura Digital; Militancia; Sociedad Civil.

EL USO DE LA TECNOLOGÍA DIGITAL COMO PROBLEMÁTICA SOCIO-JURÍDICA

a. Si bien en términos generales la tecnología digital suele ser considerada como técnicas (medios y procesos) que se basan (o se expresan) en conceptos matemáticos (numéricos) binarios y que describen objetos con dígitos con un considerable poder para comprimir cantidad de información en diferentes dispositivos de almacenamiento y que además, pueden conservarse y transportarse fácilmente. Se destaca como referente al permitir realizar cálculos matemáticos complejos analizando grandes cantidades de datos (o información) en un breve período de tiempo.

De manera que la tecnología digital –y de manera específica la Inteligencia Artificial- ha transformado la forma en que las personas interactúan, se ha variado el usual proceso de interacción social alterando la dinámica misma de la comunicación, de las formas de socializar y/o educar como la dinámica misma del

proceso de gestión en el trabajo cotidiano. Por lo que podemos afirmar que ha cambiado los estilos de vida de todos sin siquiera darnos cuenta al “naturalizar” o “normalizar” las nuevas dinámicas en las relaciones sociales.

Dudas no caben, la cultura digital ha sido durante estas últimas décadas la protagonista dentro de todos los avances, progresos y descubrimientos modernos cuya principal función es –en apariencia- optimizar y mejorar la calidad de vida los sujetos y actores sociales a partir de diferentes herramientas y recursos científicos que permiten elaborar variados productos tecnológicos. Esto conlleva que, de manera residual, impere una cultura mecánica y analógica y de manera prevaeciente se instala y se proyecta - con un turbador futuro por el potencial mismo de las nuevas tecnologías- todo aquello que es digital, lo que nos permite expresar nuestra realidad a partir de números (en lo básico, con los dígitos 0 y 1), considerado esto como una forma mucho más sencilla de hacer las cosas, y con muchas más alternativas y posibilidades de control.

b. La tecnología digital en las Instituciones Jurídicas es un fenómeno social que produce una notable variedad de consecuencias sociales problemáticas por diferentes razones: i. cobra sentido un análisis –desde la interdisciplina- de múltiples dimensiones donde se destaca el intento por optimizar la comprensión del sentido de la acción, decisión de los actores y el impacto de las mismas; ii. permite el proceso de reflexión transnormativa, al apelar a un sistema complejo, multidimensional- ya que el presente fenómeno no es lineal; cuenta con diferentes matices, posibilidades, con numerosas fases y procesos adaptativos, donde existen distintas manifestaciones de la diversidad y las formas peculiares de hechos socio-culturales en relación con la política jurídica contextualizada por el tiempo y el espacio; y iii. facilita la comprensión de las variadas dimensiones que al ser utilizadas para esos estudios y análisis desafían el sentido común, invitan a tener presente la incertidumbre y lo indecible (conductas y estructuras mutan, son dinámicas, intervienen sentidos, motivos, intereses, necesidades numerosas).

Los motivos son varios para identificar la cultura digital como un fenómeno social problemático de alto impacto en el campo

jurídico; por tal motivo se destaca la Sociología Jurídica al estar provista de diferentes herramientas teórico-empíricas que permiten que el conocimiento científico de dicho fenómeno se pueda hacer extensivo a compromisos con causas intelectuales consideradas prioritarias y urgentes. Esa disciplina –en el campo jurídico- tiene una notable ventaja debido al hecho de contar con instrumentos de análisis que permiten develar las estructuras más profundas enterradas de los “diversos mundos sociales” y que constituyen el universo social actual –con causas y consecuencias-. Se trata de recurrir a esta disciplina con el objeto de asir instrumentos para visibilizar mecanismos sociales, culturales y jurídicos (que tienden a asegurar la reproducción o la transformación de prácticas, dinámicas, situaciones, con una notable pluralidad de texturas socio-jurídicas) que suelen ser considerados de tipo periféricas o encubiertas para las disciplinas ortodoxas, tradicionales y formales típicas del campo jurídico (vg. “las disciplinas codificadas”)

c. En este caso, abordar la Inteligencia Artificial, cobre sentido al revisar, introducir y explorar el inquietante contexto social de los algoritmos utilizados para dirigir, vigilar y controlar lo

que en alguna época fue la diversidad de opiniones y la pluralidad de voces; algoritmos que en la actualidad se presentan como una condicionante de la “democracia compleja” y obstáculos a la presencia de constructores de acuerdos y de principios relacionados a una ética de prácticas comunitaria del consenso.

Surgen, entonces, un “ecosistema tecno-cultura” de carácter cambiante, dinámico donde se pueden observar tendencias, tensiones e inconsistencias en lo referente al desplazamiento de un “intercambio, discusión y consenso comunitario” producto de las prácticas que se producen y reproducen y el advenimiento de distintos escenarios futuros con una inquietante variedad de prácticas tipo totalitarias, autoritarias.

El uso y las soluciones de Big Data se podrían identificar, entonces, con asegurar la simplificación y la reducción de debates democráticos en un contexto social relacionado con el pluralismo cultural y legitimado formalmente por una notable variedad de normas, principios y garantías legales-formales de una cuestionable y, tal vez, insuficiente efectividad. Por numerosos motivos y razones de la vida cotidiana, la problemática socio-jurídica del uso político-administrativo de la tecnología digital en la consolidación de la

manipulación de las Instituciones Jurídicas es preocupante. Parecería que en el siglo XXI emergen procesos identificados con simplificar y controlar la “diversidad discursiva”.

Por tal motivo, si bien existe un aumento de la calidad y las cualidades de la información y comunicación a partir de la instalación y las consolidación de las Tecnologías de la Información y la Comunicación (TICs), coexisten además consecuencias negativas en lo referente al acrecentamiento de la segmentación social por el uso limitado, manipulado de datos; es así como dicha tecnología suele generar consecuencias disfuncionales supuestamente no queridas, tampoco esperadas porque, más allá, de ahondar la desigualdad y contribuir notablemente a la descomposición social hacen que se proyecte de manera notable hechos sociales referidos a la “cancelación” (bloqueando el debate diverso y la posibilidad de construir consensos comunitarios) típicos de sociedades con dinámicas políticas relacionadas con el “ciber-totalitarismo”.

EL “ECOSISTEMA TECNO-CULTURAL”: DE LA CIBERMILITANCIA A LA CANCELACIÓN DEL DEBATE

a. Hasta hace algo más de dos décadas

las personas aceptaba de manera pasiva lo que disponían los dirigentes. En la actualidad el cuestionamiento se da de manera prevalectante, definiendo toda una época, la población cuenta con herramientas que no dependen de nadie para expresarse. En las últimas décadas se agudiza la crisis de la vieja política entendida como reparto de ventajas entre grupos que lotean el poder. Muchas personas aprendieron a relacionarse directamente con otros, criticó a sus dirigentes, se percató de las limitaciones de los líderes mundiales, accedió a nueva información.

Casos varios de desobediencia y rebelión que necesitaban ser conducidas y contenidas surgieron en el presente siglo (vg.: un caso notable es el denominado “Primavera Árabe”) donde el proceso de concientización de la identidad colectiva adquirió fuerza a partir del uso de diferentes dispositivos y aplicaciones de las redes sociales.

Nacería y se consolidaría lo que se podría denominar “la ciber-militancia” o el uso de Internet para el activismo político que implica conocer problemas, toma de decisiones, creación de lobbys para influir en los ciudadanos, generar prácticas de voluntariados en la política de cada país. La “ciber-militancia” abarca todas las formas del software social; se debe incluir

en este proceso de visibilización y exteriorización de malestares sociales y culturales varios tópicos: actividades de periodismo, uso de blogs, búsqueda de fondos, construcción de organizaciones y voluntariado para fortalecer la sociedad civil en contextos democráticos y de un profundo pluralismo y dialogo intra-societario. Por lo expuesto los actores sociales se organizaron en red donde el liderazgo es compartido, cada sujeto tenía algo que decir, todos los integrantes de la sociedad civil querían ser partícipe de los procesos sociales que se producen en lo real y en lo virtual. Es importante señalar que no existió el control que busque silenciar voces, en la “ciber-militancia” el “ciberespacio” era (y tal vez es) un descontrol. La hiper-conectividad entretejidas de redes y nueva forma de participación social, hicieron implosionar la forma usual de hacer política. De esta manera al introducir en el campo jurídico el fenómeno del “woke” (despierto, consiente, iluminado y, por lo tanto, comprometido con el cambio) se intentó repensar, desde el uso de la Inteligencia Artificial, la importancia del valor de la Big Data y el uso que las gestiones de gobierno (y sus operadores) termine dándole.

b. Desde la primera década del siglo XXI

se acrecienta el “filtro burbuja” o “mundo amigable” en las redes sociales, situación identificada con una tercera etapa en la evolución de redes, dispositivos y aplicaciones (Gerlero, 2018, p.91). En dicha etapa los sujetos sociales viven interactuando virtualmente en pequeños mundos amigables que requieren la constante aprobación de los integrantes de su red de relaciones; sujetos y agrupamientos que se resisten a “otros” datos que confronten con sus visiones; son actores que necesitan la constante confirmación de su amigable entorno que actúa como burbuja.

Es posible que todos estos fenómenos se profundizaron en el contexto del Aislamiento Social, Preventivo y Obligatorio (ASPO) durante la pandemia (Sars-CoV-19).

Tal vez una forma actual y efectiva de encauzar la disidencia espontánea sea construyendo discursos y procesos simbólicos considerados “políticamente correcto” para sectores con pretensiones hegemónicas (también auto-denominados “contra-hegemónicos en la construcción de un exogrupo rival-enemigo) con el fin de instalar: i. una mirada simplificadora y emotiva de la realidad parcial, ii. un relato legitimado en dudosas epopeyas pretéritas que sirve como fundamento de decisiones y acciones, iii. la búsqueda

constante para imponer lo correcto y veraz al resto de una estructura socio-cultural (vg.: la aparición del *troll-militante*), y la cancelación del “otro”, del pluralismo socio-cultural y sus manifestaciones.

Explorar el fenómeno social de la “cancelación” (también conocido como negación, cultura de la acusación/denuncia o “restricción del debate”) en las redes sociales como formas referidas a variantes de la vigilancia y el control como, además, de manipulación de los datos digitales, resulta de central importancia para establecer cómo serán referenciadas y aplicadas las Instituciones Jurídicas. No deja de ser relevante el poder disponer - sin protocolos públicos- de la acumulación de datos digitales y de las múltiples alternativas que configuran la Inteligencia Artificial.

Tal es así que con el supuesto afán de utilizar un lenguaje simplificado que cierre los debates de nuevas construcciones, distintas prácticas y acciones, se toman medidas políticas de índole “verticalistas” (decisiones del poder ejercido desde la jerarquía y que pueden ser consideradas autoritarias al cancelar el debate). Claro está: la democracia implica deliberación donde las diferentes razones deben ser escuchadas, en cambio el verticalismo

refiere a decisiones y acciones inconsultas, inapelable y de carácter “paternalista”. Una sociedad civil fuerte, con una democracia de alta intensidad pide escuchar y ser escuchada para buscar puntos de encuentros, para construir puentes y buscar convencer. Lo vertical refiere a sorprender, impugnar y rechazar para disuadir, vencer y anular.

Tal vez, para algunos actores, una forma efectiva de encauzar la disidencia sea la construcción verticalista; en épocas de la cultura digital esa construcción queda en manos de fervientes militantes que comulgan con una epopeya que sirve para instalar e insistir con lo “políticamente correcto y valioso”, con la cancelación del pluralismo socio-cultural y sus manifestaciones. Esto ocurre posiblemente cuando la pluralidad de los actores sociales dejan de reconocerse como responsables de una articulación que busca el bienestar y calidad de vida de cada sujeto.

c. En este “ecosistema tecno-cultural” el paso de la ciber-militancia (*woke*) a la cancelación del debate (*cancel culture*) se viene sosteniendo desde diferentes textos teóricos y empíricos. Como se viene afirmando en “Haciendo Sociología Jurídica” (Gerlero, 2018) se comienza a

experimentar fenómenos sociales con alta incidencia en las Instituciones Jurídicas; fenómenos que se identifican con una “fatiga en los lazos comunitarios y democrático liberal” con la necesidad de hacer prevalecer una conciencia emotiva, afectiva e individual basada en leyendas o ficciones arbitrarias seleccionadas desde el poder verticalista. Es así como se pierde el interés y el sentido de pertenencia a diferentes agrupamientos sociales que dan textura y matices a la diversidad socio-cultural, base de una sociedad civil fuerte. La nueva sociedad y cultura simplificada –carente de matices y complejidades- con rasgos de “nueva” hegemonía produce un “cansancio social” o agotamiento de los actores sociales en el uso alternativo de las herramientas culturales y jurídicas que crean y, además, se presentan como un referente del necesario consenso comunitario para mantener estructurada, de manera plural y diversa, la sociedad. Esto sucede, de manera destacada, cuando el sujeto pasa a sentirse como un engranaje de una maquinaria estructura verticalista en donde no participa con decisiones ni acciones propias. Le gana el “desaliento y descredito referido a las instituciones” al dejar de condensar intereses y necesidades de distintos agrupamientos y de sujetos en particular y de no

responden la multiplicidad y complejidad de expectativas que tienen los agrupamientos y actores que conformaban la sociedad civil amenazada.

d. Lo expuesto implica un referente del paso definitivo de la “Tecnología de la Información y la Comunicación” a la “Tecnología de la Información y el Control”. La emergencia de este último tipo de sociedad transforma la existencia de los actores; prevalece la existencia electrónica y, como espacio de encuentro, cualquier dispositivo que los permita y facilite; esta situación lleva a modificar patrones de comportamiento ante la producción, circulación, consumo e interpretación de la información; la garantía de la existencia es el estar conectado a los dispositivos electrónicos que configuran la realidad de cada sujeto y conforman nuevos sentidos a la idea de “comunidad” producto de un notable reduccionismo narrativo por la militancia de agrupaciones verticalistas.

El paso de una concepción o forma de considerar esta tecnología a la nueva deja en evidencia la fragilidad de la cultura digital cuya fuerza había residía en la promesa de una comunicación que prometía mayor libertad y pluralismo

democrático; ahora dicha tecnología opacó sus funciones.

Esta opacidad se encuentra garantizada por los dispositivos que orientan al observador en complejos algoritmos, los límites de dicho examen que condicionan la reflexión, las numerosas orientaciones que determinan la mirada del ciudadano, situaciones que intimidan y apabullan sujetando todo posible libre abordaje; no se trata de los filtros culturales de cada actor (en su socialización o educación) sino de las operaciones que tienden a encubrir situaciones; esto es la opacidad: es impedir ver los datos que se están buscando manipulando hechos y evaluación de los mismos y, además, cancelando la disidencia

LA CULTURA DE LA CANCELACIÓN Y LA LEGITIMACIÓN POLÍTICO - ADMINISTRATIVA

a. De una “militancia activa” (*woke*) a su “cancelación” (*cancel culture*) solo existiría, en un trabajo de campo, debido a una posible variable interviniente: la decisión de agentes de gobierno (en la gestión, en las decisiones y acciones políticas) legitimada en una narración o mito de una épica pretérita (un proyecto que puede ser considerado hegemónico pero que es un relato simplificador de la multiplicidad de lecturas e

interpretaciones) donde las versiones alternativas no son aceptables y acciones que son acompañada por el fervor lo que se podría llamar el “*troll-militante*” con un posible ilimitado acceso a la acumulación de datos y a las herramientas que conforman la Inteligencia Artificial.

Es así como de un activismo y militancia intensa –que marca una época en la militancia digital y en un fervor por la diversidad de discursos y planteos que buscan una estructuración social y cultura diversa- se pasaría a la prevalencia de una suerte de clausura de la pluralidad, instalándose, posiblemente, una cultura del odio, de la revancha y de la venganza; de todos modos se trata de acción y reacción producto de la simplificación de la información y de la manipulación de la dirigencia y corporaciones de diferentes orientaciones político-ideológicas. Ese odio construido, tal vez, en manipular datos en el “filtro-burbuja” impide el razonamiento y prescinde de la reflexión en el debate de ideas y en la construcción de consenso y acuerdos comunitarios que fortalezcan la sociedad civil.

Para remarcar: en el paso del “*woke*” a la “*cancel culture*” se produce un fortalecimiento del “nosotros” y del “ellos” que, enfrentados, construyen un campo de pertenencia que rechaza cualquier tipo de entendimiento o posible consenso

dando lugar a un escenario en el que la polarización se potencia en frustraciones personales y tensiones sociales varias.

Esta perspectiva institucional disfuncional (consecuencias de hechos socio-culturales que perturban la estabilidad social) produce un aumento del miedo en sectores de la sociedad, profunda desconfianza y resentimiento hacia “el otro”; se da el peligroso fenómeno donde un agrupamientos va siendo cada vez menos receptivo a intereses, necesidades y expectativas del “otro”. Para beneficiarse de este temor hay quiénes no dudan en encender ciertos sentimientos hostiles en la población hacia esos sectores sociales. El objetivo es deshumanizar al otro e identificarlo (manipulando situaciones e información) con valores negativos como forma de buscar una legitimación al momento de demostrar un desprecio o rechazo ante el sector que puede ser repudiado solo por una construcción política-ideológica.

b. En este inquietante contexto los algoritmos para dirigir y, por sobretodo, vigilar y controlar lo que en alguna época fue la diversidad de opiniones y la pluralidad de voces limitarían la “democracia compleja” (y la presencia de constructores de consenso y de principios

como, además, de prácticas comunitarios). El uso y las soluciones de Big Data en contextos de “cancelación de los debates” desacreditando al “otro” negando sus demandas y su existencia se podrían identificar, además, con asegurar la simplificación y la reducción de debates democráticos relacionados con el pluralismo cultural.

El sistema democrático (muchas veces débil por anular o silenciar voces disidentes) con gestiones que disminuyen la intensidad de la construcción de consenso suelen generar una crisis y un menoscabo de legitimidad de Instituciones que son consideradas valiosas y que tenían fines específicos en sociedades estables y consolidadas.

Limitar la diversidad y la pluralidad, aunque se violen un sinnúmero de derechos, lleva a explorar el fenómeno de la “cultura de la cancelación” (o *cancel culture*) como un posible y desesperado intento de vigilar y controlar lo que circula por las redes sociales (con variantes reaccionarias del ciberactivismo); esto podría ser de vital importancia por la amenaza que se cierne sobre el pluralismo en el campo jurídico.

El punto de partida para pensar en un análisis teórico de la “cultura de la cancelación” sería considerar las

prácticas, discursos y actuaciones sociales institucionalizadas en un momento determinado como las hegemónicas, desplazando las demás a los márgenes o bordes de la misma sociedad; de esta manera se estaría en presencia de situaciones de violencias simbólicas al ignorar; construir hegemonías (o contra-hegemonías según la postura en el análisis) implica silenciar u ocultar una pluralidad de intereses, necesidades, situaciones y fenómenos. Una forma efectiva de esa violencia, entonces, es simplificando y escondiendo diferentes saberes, discursos y situaciones sociales; es una forma de oscurantismo posterior a la modernidad y producto directo de la dinámica de las mencionadas tecnologías.

c. Existe una peligrosa posibilidad de que se instalara así un nuevo parámetro de prácticas en el Campo Jurídico: habría menos derecho a la intimidad, menos respeto a la vida privada, pero más seguridad y control, aumentaría el disciplinamiento y las prácticas normalizantes promoviendo ciudadanos más dóciles, condescendientes, apáticos y timoratos; es el uso de la “seguridad pública o nacional” suele ser la legitimación en ciertas gestiones de gobierno o la de un funcionario; implica de manera directa el posible uso arbitrario,

parcial, sectorial de las herramientas que conforman la Inteligencia Artificial.

Es institucionalizar una suerte de “estado de excepción permanente” donde se pone el acento en la construcción de un relato, una narración “verosímil” con instituciones que sean un producto combinado de discursos contruidos a base de mitos, leyendas, versiones limitadas del liberalismo jurídico (libertad, igualdad, división de poderes, entre otros ejemplos) a partir de mitos lo más verosímil posible y que son percibida como posibles realidades por la mencionada Sociedad Disgregada y Compleja; donde se produce información y se estructuran instituciones que van más allá de las necesidades y expectativas reales de los distintos actores sociales. Muchas veces esas versiones de Instituciones se encuentran vacías y carentes de sustancia, de contenido, llenas de relatos contruidos a partir de la tergiversación de diferentes hechos sociales. Suele haber una apelación constante a lo emotivo y a las creencias personales. A modo de ejemplo tomar categorías como “la seguridad nacional” es una construcción, es el resultado de un proceso social deliberado, una construcción política y corporativa -en un momento y en situaciones consideradas oportunas- que necesita ser abordada con

urgencia por ser consideradas “peligrosas” o “amenazantes”; esa categoría es producida por una narrativa de agrupamientos con poder. El recrear hegemonías implica no solo cancelar refiere, además, a la búsqueda de la construcción de una seguridad mediante la imposición de un discurso, narración o relato. De esta manera no se tienen en cuenta hechos (y su complejidad) no importa si lo que describe y promociona responde a la compleja realidad de situaciones sociales problemáticas; son sociedades e instituciones “performativas” (o hechas a partir de las palabras y no a partir de reales necesidades y situaciones concretas, se trata de realidad construidas discursivamente) ya que no se construyen sobre hechos, sino apelando a la sensibilidad, a la pasión, a la compasión, a una extensa gama de emociones (vg.: un enemigo real o simbólico, el otro, el distinto). Esto se sintetiza de la siguiente manera: para construir una nueva realidad –funcional a dichas administraciones y corporaciones- hay que crear un nuevo lenguaje, un espectáculo que represente a lo que podría ser verdad en términos objetivos, un nuevo discurso hegemónico donde el *troller* militante contribuye a cancelar la diversidad y la disidencia. El sujeto, las necesidades, las problemáticas complejas desaparecen y son reducidas a

un discurso creíble para la militancia.

UN RESULTADO PREVISIBLE: EL “CIBERTOTALITARISMO”

a. Por las razones arriba expuestas y en el contexto de combinar funciones y disfunciones de la Tecnología de la Información y la Comunicación (TICs) resulta importante destacar el alto impacto de las mismas en la calidad institucional. Las posibilidades virales producto de la cultura digital pueden ampliar los mensajes implícitos, los relatos y, en su defecto, realizar nuevas lecturas sobre la efectividad, la vigencia, la racionalidad, la funcionalidad y la legitimidad de las Instituciones Jurídicas.

Deseado, o no, la tecnología (abarcando numerosas herramientas, técnicas y procesos producto de la acumulación de datos y de la implementación de algoritmos) se hace presente en la manipulación en la vida diaria incluso para legitimar decisiones y acciones en la gestión administrativa.

Es así que todo sistema social convenientemente institucionalizado necesita legitimarse para subsistir. Desde lo formal el Estado debe garantizar la integridad física, económica, social y cultural de sus ciudadanos, también tiene que velar por su propia supervivencia, porque un estado fuerte es del interés de

todos. En la realidad cotidiana prevalecería una deslegitimación de las Instituciones que por diferentes razones, algunas de ellas mencionadas tangencialmente en el presente texto, se encuentra cuestionadas por su propia ineficiencia; además se percibe la desaparición de las referencias sociales, supuestamente, sólidas indicadores con numerosas ambivalencias y contradicciones; existen diferentes textos que refieren a un Estado indefinido, impotente y negador, en vías de ser directamente un Estado fallido. Es decir, uno que ya no es capaz de responder a las necesidades más básicas de la sociedad, y que no se mantiene como un actor creíble a nivel nacional e internacional.

b. Frente a lo expuesto, en el paso de un notable ciber-activismo (*woke*) que, con el tiempo y en devenir político, termina en prácticas de cultura de la cancelación /acusación/denuncia o “restricción del debate”, se estaría frente a una muy posible situación considerada como problemático: la presencia de un fenómeno socio-político identificado con el “ciber-totalitarismo”

En la cultura digital, del paso del uso de las redes sociales para visibilizar

problemas sociales y culturales periféricos y aumentar la participación y el compromiso de la sociedad civil (*woke*) se pasa a un nuevo momento en donde ese activismo producto de un compromiso político se radicaliza, “cancelando” debates que construyen consenso. Esta secuencia o evolución terminaría con la consolidación de un “cibertotalitarismo” limitando o anulando la valía de la sociedad civil.

Se podría intentar rescatar características que definen el cibertotalitarismo: frente a condiciones de emergencia e incertidumbre social y política en vez de usar alternativas relacionadas con consenso se toman decisiones y se aplican acciones que son producto de la arbitrariedad en la gestión administrativa, donde los derechos se vuelven precarios y relativos a situaciones de “excepcionalidad-permanente”, se busca la efectividad de la vigilancia y el control en la aplicación racional de un proyecto hegemónicos y verticalistas, y a través del eficaz uso de la tecnología digital que incluye inteligencia artificial y la posibilidad de influir en la vida socio-política utilizando algoritmos.

Hay un desplazamiento de la presencia de democracias complejas que articulan a la diversidad, por democracias de baja intensidad con pretensiones de simplificar

la realidad, examinando salida superficial en el antagonismo: amigo-enemigo.

c. Las “condiciones de emergencia” siempre implican algún tipo de suspensión del Estado de Derecho y un resurgimiento de una autoridad del Poder Ejecutivo por sobre los demás poderes. Se trata de un tipo de sociedad en donde, como nuevo paradigma del campo jurídico, se vuelve rutinaria la posibilidad de suspender los derechos fundamentales en determinadas circunstancias en las que la supervivencia del Estado mismo se puede ver comprometida por graves alteraciones de su seguridad interior o exterior, del normal funcionamiento de las Instituciones o del normal ejercicio de los derechos y libertades, así como seriamente amenazada, peligros y/o riesgos para la población. En determinados supuestos la vigencia de los derechos puede cesar total o parcialmente.

El comenzar con excepciones por situaciones consideradas de riesgos o emergencia que se construye –entre dirigentes, políticos y corporaciones- un sentido alternativo de Estado, se escenifica un tipo de gestión y percepción del Estado desde una suerte de política de la “gestión o pedagogía del terror, del pánico o -por sobre todo- una gestión de

la sospecha”; esto sucede cuando a las personas se les recuerda la mortalidad desde el peligro posible, la amenaza, el riesgo (aumento de la pobreza y la desocupación, inmigrantes ilegales, enfermedades pandémicas, ataques terroristas internos y/o externos). Situación está que implica, muchas veces, un abandono de la probabilidad real de la inminencia de cierto fenómeno; algunas reparticiones administrativas promueven situaciones imaginarias con el objeto de animar a distintos actores sociales a ser condescendientes al control por el pánico y la alarma con supuestas consecuencias para sus vidas y bienes.

Parce, entonces, que en este tipo de sociedad las prácticas estructurantes referidas al Estado se identifican con las agencias de control informático, de captura de enormes cantidades de datos. Es posible que el Estado, como entidad política, territorial, solo se mantenga en actores identificados con los “soberanistas” o movimiento político que propugna la soberanía de un territorio, esto puede ser identificado con sectores progresistas y/o conservadores, pero todos reaccionarios.

d. Resulta un dato notable, para futuros trabajos teóricos, alrededor de 2011 se

construye un nuevo tipo de arquitectura informática: una nube que permite a cualquier “agente o guardián del sistema” independiente de su ubicación física, acceder a los datos que necesitare y hacer búsquedas en ellos de lo que necesitare para hacer efectivo el control y con la posibilidad real de alterar de manera irrevocable las vidas de ciudadanos que hasta hace una década contaban con la garantía de la aplicación y protección de sus derechos. A partir de las denuncias de Snowden (Gerlero, 2018, p.103) se consolida así una dimensión sofisticada del capitalismo: el de la vigilancia. Situación tal garantizaba, no solo la limitación del Estado de Derecho tal como se conocía en la estructura de la Sociedad Nacional, perfeñada en el modernismo sino, además, una concepción de poder en donde se desplaza la función social de las Instituciones Jurídicas por una “tiranía tecnológica” también considerada como una vertiente de “Cibertotalitarismo” donde las herramientas digitales están al servicio del control y la vigilancia y, de ser necesario, de la cancelación.

e. Es de repensar las funciones de los operadores del derecho en el campo jurídico; se promueve –frente a la cancelación- recuperar el valor social y

comunitario de una vinculación o construcción colectiva que implica dar respuestas a una forma de pensar y actuar que tenga como centro no solo al individuo, a este en comunidad; no limitado a gestiones, acciones y/o proyecto político.

Parecería que con la fragmentación social y cultural (posible negocio de la dirigencia y corporaciones) y la consabida pérdida de prestigio de las Instituciones es necesario nuevas aceptaciones y pactos que al menos contengan la voraz dinámica de la cultura digital del siglo XXI.

La sociedad civil se apoya en esa red de derechos y acciones que se enmarca en las instituciones, organizaciones y asociaciones, esto es todo tipo de agrupamiento social que tiene como objeto expresar interés, necesidades y derechos de los actores. La sociedad civil no sólo es importante para defender las necesidades de las personas ante sus agencias de gobiernos y sus grupos asociados (vg.: empresarios) sino para hacer que distintos gobiernos y sus asociados rindan cuentas en relación con el cumplimiento de sus compromisos asumidos y los protocolos públicos utilizados. El uso de la Inteligencia Artificial y todo lo que conlleva el manejo de la Big Data depende, por lo tanto, de la ética y el compromiso de la gestión

administrativa; ese uso depende de la responsabilidad social y civil con la pluralidad social.

Una nueva ética del consenso con base comunitaria con protocolos de control en el uso de las herramientas que conforman la Inteligencia Artificial, alejado del voluntarismo político, podría ser el resultado de una construcción desde la gestión de gobierno que permitiría el desplazamiento de la cultura de la cancelación y el refortalecimiento de la diversidad democrática y la valía de las actuales Instituciones.

BIBLIOGRAFÍA:

- Gerlero, M. Liceda E. y Lezcano J.M., Redes Sociales y derechos, Buenos Aires: Visión Jurídica, 2019.
- Gerlero, M., Haciendo Sociología Jurídica, Buenos Aires: Visión Jurídica Ediciones, 2018.
- Gerlero, M., Lecciones de Sociología Jurídica, Buenos Aires: Ediciones Jurídicas, 2016.
- Gerlero, M., Sociología Jurídica y los nuevos movimientos sociales, Buenos Aires: Visión Jurídica, 2011.

LA ERA DE LOS ALGORITMOS ¿ENEMIGOS O ALIADOS?²³

Ariadna Luján Martínez²⁴

Francisca Ojeda Campos²⁵

RESUMEN

Como sociedad estamos pisando terreno desconocido en lo que a nuevas tecnologías se refiere. Las potencialidades de la inteligencia artificial (IA) son innumerables, sin embargo, no son infalibles y los sesgos algorítmicos son uno de los grandes desafíos que presenta. En ese contexto, hemos desarrollado las bases de un protocolo para alcanzar una IA con sello ético y enfoque social.

El mayor reto es comprender que la IA, no solucionará automáticamente problemas estructurales. Los daños causados por algoritmos son de responsabilidad humana y la IA es una herramienta que se inserta en un determinado contexto y cuyo funcionamiento y éxito dependerá de las personas.

Una IA responsable es posible, pero requiere de educación, la fijación previa de parámetros de uso, y el desarrollo de marcos técnicos, de monitoreo de los sistemas, como también, una dimensión humana, que involucre a los distintos actores sociales que han de beneficiarse con ella.

Palabras clave: Inteligencia artificial – Sesgos – Interdisciplinariedad – Descentralización – Colaboración.

23 Enlace al video <https://youtu.be/ESpnji3-kBg>

24 Estudiante avanzada de la carrera de Derecho de la Universidad Nacional de Cuyo. Email: ariadnalujan41@gmail.com

25 Abogada de la Universidad Adolfo Ibáñez, Chile. Email: fojedacampos@gmail.com

INTRODUCCIÓN

Como sociedad estamos pisando terreno desconocido en lo que a nuevas tecnologías se refiere. Las potencialidades de la inteligencia artificial (IA) son innumerables, sin embargo, no son infalibles y los sesgos algorítmicos son uno de los grandes desafíos que presenta.

Los más fatalistas ven a la IA como una enemiga, creyendo que su implementación devendrá en el reemplazo de los humanos por las máquinas. Los más escépticos, piensan que aún se trata de ciencia ficción, del futuro. Por el contrario, nosotras creemos y buscamos promover una mirada optimista, que percibe a la IA como una herramienta que complementa y facilita labores humanas.

Hoy, el mayor reto es comprender que la IA, no solucionará automáticamente problemas estructurales. En ningún caso desconocemos los riesgos ni la posibilidad de errores en el desarrollo de la misma, pero el foco ha de dirigirse a los desafíos que se observan, y discutir las posibles soluciones.

Nuestro objetivo es plantear las bases de un protocolo para el uso de sistemas

algorítmicos basados en IA, inspirado en las indicaciones de la Comisión Europea, en las Recomendaciones de la Red Iberoamericana de Protección de Datos, las investigaciones de autores como Juan Corvalán y el trabajo realizado por científicos de datos que también creen posible una IA ética y responsable.

DESARROLLO

“La dificultad radica, no en las nuevas ideas, sino en escapar de las viejas”²⁶.

Previo a desarrollar nuestra propuesta de bases para un protocolo, creemos necesario precisar algunos conceptos.

¿Qué son los algoritmos?

Son un conjunto de instrucciones o reglas definidas, ordenadas que permiten solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo tareas o actividades, siguiendo pasos sucesivos, llegando a un resultado final (obtener patrones). Estos algoritmos, son entrenados con datos, y tal como afirma Corvalán (2020) permite la vinculación entre algoritmos y Machine learning: El término *aprendizaje automático* se refiere

26

a la detección automatizada de patrones significativos en los datos.

Es importante remarcar que cuando hablamos de sesgos algorítmicos debemos saber que los mismos reflejan los valores de los humanos que están implicados en la codificación, recolección de datos para entrenar al algoritmo.

Por lo expuesto, es que creemos que cualquier desarrollo responsable de la inteligencia artificial, debe contemplar, un ámbito humano y un ámbito técnico.

Como mencionamos anteriormente, siguiendo los lineamientos del “Libro Blanco sobre Inteligencia Artificial” de la Comisión Europea y las Recomendaciones Generales de la Red iberoamericana de protección de datos personales, ambos documentos publicados durante el 2020, es que llegamos a las siguientes proposiciones:

Ámbito Humano o Ético

Los sistemas son realizados por humanos, por tanto, el avance y desarrollo de la IA debe ir necesariamente acompañado de una formación tanto de quienes crean los sistemas, como de quienes toman las decisiones de implementación, y de los destinatarios o usuarios. Formar equipos

con un alto grado de conciencia en materia de ética es fundamental, de manera de fomentar el pensamiento crítico y cuestionador, y así poder crear sistemas que sean coherentes con los valores e ideas de la sociedad actual.

Por otro lado, los seres humanos naturalmente tenemos sesgos; para disminuir esto y poder avanzar en la educación y formación digital debemos formar un ecosistema de IA que acerque las ventajas de la tecnología a la sociedad, lo que debe hacerse desde distintos ámbitos y considerando los diversos actores que pueden estar involucrados.

Desde el sector público, se debe trabajar para asegurar el acceso de datos y a la infraestructura informática. Además es necesario un marco político que fomente la investigación y la innovación. Promover la educación digital desde los primeros niveles de educación hasta los universitarios, acompañado de regulación o protocolos que sean flexibles, ya que la necesidad de adaptación y re adecuación será constante con los avances que existen día a día.

Desde el sector privado, es necesario que el mismo pueda participar en la agenda de innovación e investigación (según sugiere

el Libro Blanco) lo cual creemos que es efectivamente necesario. Pero además contar con participación ciudadana, facilitando el acceso a la información y que la misma sea clara, promoviendo la transparencia de los algoritmos, la consulta pública a la hora de hacer regulaciones y la promoción de softwares de código abierto.

Interdisciplinariedad²⁷: En palabras simples, significa que en el proceso de desarrollo de sistemas algorítmicos exista una “combinación de actores, elementos y valores de distintas áreas del conocimiento” (Cevasco, Corvalán y Fevre, 2019). Este es el factor clave de nuestra propuesta, sin colaboración, sin aportes de distintas áreas todo lo demás no será exitoso.

Ámbito Técnico²⁸

El ámbito humano debe necesariamente complementarse con protocolos de funcionamiento y revisión de los sistemas, lo que hemos denominado área técnica, es decir, a realizarse en el proceso de

²⁷ La Real Academia Española lo define como “Dicho de un estudio o de otra actividad: Que se realiza con la cooperación de varias disciplinas”.

²⁸ Como mencionamos anteriormente, el objetivo de este documento es hacer una breve reseña de nuestra disertación en el Congreso, por lo cual para ampliar conocimientos humildemente los dirigimos al canal de youtube “ElDerechoinformativo TV” donde podrán profundizar lo que aquí tratamos.

desarrollo del algoritmo o en el post procesamiento del mismo.

Elegimos dos sistemas de auditoría de modelos de machine learning, enfocados en reconocer y mitigar los sesgos que pueden introducirse en los sistemas de diversas formas y en distintas etapas del desarrollo del modelo.

a)

Es un paquete de Python (lenguaje de programación) desarrollado por Microsoft, que implementa algoritmos para detectar problemas de equidad de grupos de modelo de aprendizaje automático y a su vez mitigar injusticia. Se pueden utilizar algoritmos para mejorar el modelo durante el entrenamiento, pero también, algoritmos de post-procesamiento para mejorar modelos ya existentes. Funciona a través de un panel de evaluación para evaluar cómo las predicciones de un modelo afectan a distintos grupos y a su vez, utiliza algoritmos de mitigación para disminuir la injusticia en la clasificación. Además mide la dependencia de un modelo de sus entradas cambiandolas, si un cambio provoca drásticamente una modificación en la salida entonces el modelo es sensible a la característica.

²⁹ Más detalles en <https://fairlearn.github.io/>

b) Modelo aequitas³⁰:

Es una herramienta desarrollada por el Center for Data Science and Public Policy for Social Good Foundation, originalmente en la Universidad de Chicago, y actualmente en la Universidad de Carnegie Mellon en EE.UU. la misma es de código abierto³¹ y permite auditar modelos de machine learning para detectar y mitigar sesgos, respecto de múltiples atributos (etnicidad, sexo, edad, etc.). Se basa en una definición de sesgo entendida como medida de disparidad entre grupos, en comparación con un grupo de referencia. A su vez, el grupo de referencia, se puede seleccionar utilizando varios criterios (los mencionados más arriba).

Lo distintivo de Aequitas es que tiene presente que sesgo y “fairness” no son conceptos absolutos y que están necesariamente vinculados al escenario al que se aplican, como asimismo al análisis y a la interpretación dentro de ese contexto. Por otro lado, pretende ser útil también a autoridades en general y no limitarse a ser entendido únicamente por personas con conocimiento técnico.

³⁰ La explicación que viene a continuación, se baja en el documento desarrollado por Saleiro, Kuester, Stevens, Anisfield, Hinksos, London, Ghani, (2018).

³¹ Más detalles en: <https://github.com/dssg/aequitas>

Una explicación más detallada del funcionamiento tanto del modelo Fair ML como de aequitas excede el objetivo de este documento, por lo cual, para aquellos que deseen profundizar en la materia, se recomienda acceder directamente a las fuentes. Lo importante es difundir su existencia y dar cuenta de que existe un interés y preocupación por desarrollar inteligencia artificial responsable con sello ético y en beneficio de las personas.

CONCLUSIÓN

Es imperativo que la implementación de sistemas de IA vaya acompañada de discusiones y capacitaciones en el ámbito humano y de auditorías a los modelos, como alguno de los que mencionamos previamente, de forma de lograr una IA que sea a la vez útil, responsable y con enfoque social.

En este sentido, resulta acertado lo que expresa Kate Crawford, de Microsoft Research, “es hora de reconocer que los algoritmos son una creación humana que hereda nuestros prejuicios [...]: nuestra IA será tan buena como lo seamos nosotros”.

Creemos firmemente que esta afirmación va de la mano de educación ética y digital de los ciudadanos, y distintos actores sociales, como mencionamos, de estados

PROACTIVOS, que no se resistan a lo que ya está sucediendo sino que desde la interdisciplinariedad y la escucha de todos los sectores busquen soluciones de las que TODAS las personas participemos. Que la IA sea potencialmente destructiva o potencialmente beneficiosa, creemos está en manos de nosotros.

BIBLIOGRAFÍA

- Cevasco, L., Corvalán, J., Le Fevre, E, “Inteligencia Artificial y Trabajo. Construyendo un nuevo paradigma de empleo”. Astrea SRL, Buenos Aires, 2019.

- Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnología (Comisión Europea), “Libro Blanco sobre Inteligencia Artificial – Un Enfoque europeo orientado a la excelencia y la confianza”, Bruselas, 2020.

- Corvalán, J, “Perfiles digitales humanos”. La Ley, Buenos Aires, 2020.

- Red Iberoamericana de Protección de Datos – RIPD-, “Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial”, 2020.

- Saleiro, P., Kuester, B., Stevens, A., Anisfeld, A., Hinksos, L., London, J., Ghani, R, “Aequitas: A Bias and Fairness Audit Toolkit”. Center for Data Science and Public Policy, University of Chicago, Chicago, 2018.

Capítulo 2 La Inteligencia Artificial y su aplicación en situaciones problemáticas

LA INTELIGENCIA ARTIFICIAL AL SERVICIO DEL MARKETING LÍMITES AL TRATAMIENTO DE DATOS PERSONALES³²

María de los Ángeles Tedesco³³

RESUMEN:

En la actualidad, existen empresas en las que su actividad comercial reside en la obtención de datos personales de particulares, como ser gustos, intereses, opiniones y elecciones en la esfera privada de sus acciones. Con dichos datos y a través de algoritmos específicos se forman perfiles de consumo y se transforman en un insumo para ofrecer servicios a otras empresas que podrán dirigir sus publicidades a un grupo determinado de interés.

Estas publicidades direccionadas, lograrán o intentarán persuadir la elección del receptor de una forma sutil, influenciándolo de elegir un bien o servicio por sobre otro. Pero en esta tarea resulta necesario establecer los límites jurídicos al tratamiento de datos personales como al consentimiento para que no resulte una manipulación maliciosa en la toma de decisiones y un avasallamiento del derecho a la intimidad, privacidad y autodeterminación informativa. Se desarrollará como es el procedimiento mediante el cual las empresas obtienen los datos personales y como obtienen el consentimiento para el tratamiento de estos.

Finalmente se concluirá con la necesidad de un cambio normativo que resulte acorde a las necesidades actuales y al avance que ha tenido la tecnología utilizada al servicio del marketing, estableciendo en el mismo limitaciones al tratamiento de datos con fines publicitarios basada en el principio de finalidad y

32 Enlace al video: <https://youtu.be/JbRfi8xT15w>

33 Abogada, Especialista en Gestión de las Instituciones (FLACSO 2017) Especialista en Docencia Universitaria (IUPFA 2018) Doctorando en Derecho (UK). Secretaria Académica Unidad Académica de Formación Profesional y Permanente Instituto Universitario Policía Federal Argentina. mail: marytedesco@hotmail.com

la forma de otorgar el consentimiento.

Palabras claves: inteligencia artificial - marketing tecnológico –datos personales
– big data – principio de finalidad

INTRODUCCIÓN: MARKETING TECNOLÓGICO Y MINERÍA DE DATOS

El derecho a la protección de los datos personales se encuentra consagrado en legislaciones de todo el mundo desde hace varios años, pero en este último tiempo ha adquirido significativa relevancia.

En el marco de la sociedad de consumo y la información, la recolección, utilización e intercambio de datos cada vez tiene mayor importancia. El impacto, alcance y penetración de la conectividad a internet en todo el mundo, la popularización y avance de los dispositivos móviles y redes sociales traen consigo un cambio de paradigma en el derecho a la protección de datos personales.

Las nuevas técnicas de análisis de datos masivos, llamados “Big Data”, han venido a dotar de nuevo sentido y conceptualización a los datos, tornándose en el centro de la estrategia comercial de las compañías de todo el mundo.

En la actualidad, existen empresas que se

dedican al “Big Data”, “Data Mining” o “Minería de Datos”. A modo de ejemplo, explicaré como funcionan algunas de ellas: colocan su tecnología no intrusiva, en espacios comunes de centros comerciales, mediante la cual se obtienen pulsaciones electromagnéticas que emiten los teléfonos celulares con el objetivo de obtener información relevante que, luego de ser cruzada con otros datos enriquecidos, pueda en un futuro ayudar a predecir la demanda, estableciendo nuevos objetivos en la atracción de nuevos y antiguos clientes.

La cantidad de datos que producimos los seres humanos se duplica año a año y a través del análisis de estos por aplicación del machine learning³⁴ permite que la inteligencia artificial aprenda a pensar y

34 Machine Learning: Disciplina científica del ámbito de la Inteligencia Artificial que crea sistemas que aprenden automáticamente. *Aprender* en este contexto quiere decir identificar patrones complejos en millones de datos. **La máquina que realmente aprende es un algoritmo** que revisa los 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. Veamos cómo funciona. recuperado de <https://cleverdata.io/que-es-machine-learning-big-data/#:-:text=Machine%20Learning%20es%20una%20disciplina.complejos%20en%20millones%20de%20datos>. El 14/06/2020

sentir como los seres humanos logrando una curva de aprendizaje acelerada.

EL CONSENTIMIENTO Y EL TRATAMIENTO DE DATOS PERSONALES

Las compañías que implementan estas técnicas de recolección y análisis de datos masivos encuentran “el consentimiento” del titular para realizar estas acciones, ya que a fin de ofrecer algún premio o beneficio o simplemente para poder conectarse a una red wifi o acceder a páginas web, el usuario debe aceptar los términos y condiciones o que la página trabaje con “cookies”. Lo que si estamos seguros es que nada resulta gratis.

El consentimiento del afectado es esencial en lo que respecta al tratamiento de datos, ya que todo banco de datos o registro ya sea público o privado, que desee tratar datos de personas físicas o jurídicas, deberá requerirles previamente su consentimiento para el tratamiento, salvo que los datos se encuentren en alguno de los supuestos legales que eximen del mismo.³⁵

35 Basterra Marcela I. “Protección de datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales.” Página 6

Para el cruce de datos obtenidos, se establece una estructura llamada datawarehouse, cuya finalidad de tratamiento es indagar en las bases de datos donde previamente las personas consintieron el tratamiento de sus datos con el objeto de obtener una nueva base de datos resultante del entrecruzamiento de datos anteriores.³⁶

En principio, cualquier técnica de data mining exigirá el consentimiento previo del sujeto afectado, no sólo para efectuar ese tratamiento, sino también para su uso con la finalidad concreta a la que se pretenda destinar. El hecho de que exista consentimiento del afectado para el tratamiento de sus datos en otros casos no significa que se pueda efectuar un tratamiento paralelo, que supondría una vulneración del principio de finalidad del tratamiento contenido en el artículo 4.1 y 4.3 de la ley de protección de datos personales.³⁷

Actualmente, las técnicas de data mining han ganado mucho con la llegada y evolución de la red. La cantidad de datos de un usuario que puede conjurar un

36 Idem ant. Pagina 8.

37 Basterra Marcela I. “Protección de datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales.” Página 9.

portal de comercio electrónico es inmensa, partiendo de los datos voluntariamente introducidos por el usuario registrado, y pasando por los hábitos de navegación que demuestre en su utilización diaria de los servicios del portal. La personalización le permite seleccionar de forma voluntaria los contenidos que son de su interés, pero asimismo permitirá a la empresa propietaria del portal conocer mejor que productos pueden ser del interés del usuario. La empresa que lleva cabo el cruce de datos o “data mining”, debería notificar el resultado al titular de los datos y en caso de no contar con su consentimiento o que el mismo sea revocado, automáticamente sacar el dato del correspondiente registro.³⁸

Cuando completamos un formulario para obtener un cupón de descuento o pasamos por distintos sistemas de supermercados las tarjetas de puntos para obtener descuentos o beneficios, estamos entregando datos a cambio de ello. Estamos informando además de nuestro nombre y apellido, datos privados, como ser gustos o preferencias por ciertos productos o ciertas marcas. La reglamentación de la norma admite operaciones de tratamiento de datos con

finés publicitarios en determinados supuestos, sin que medie el consentimiento de sus titulares. En tal sentido, se permite que en la recopilación de domicilios, reparto de documentos, publicidad o venta directa, se procesen datos personales aptos para la conformación de “perfiles” de sus titulares con fines promocionales, comerciales o publicitarios, o bien, para determinar hábitos de consumo, a efectos de desarrollar la difusión de determinados productos y servicios y poner a disposición de los titulares de los datos recolectados ofertas a medida de sus preferencias y necesidades.³⁹

Con los mencionados datos, las empresas comerciales pueden dirigir mejor su publicidad, maximizando así su eficacia y llegada al público. Para ello se utilizarán un algoritmo que permitirá predecir el consumo basándose en una base de datos con información sobre muchos clientes para los cuales observa su patrón de consumo.

38

39 RIGAUX, François, “La protection de la vie privée...” p. 597, citado por PEYRANO, Guillermo F., Régimen Legal de los Datos Personales y Hábeas Data. Comentario a la ley 25.326 y a la reglamentación aprobada por Dec. 1558/2001, Lexis Nexis, Depalma, Buenos Aires, 2002, p. 250

EL PRINCIPIO DE FINALIDAD COMO LÍMITE

El supuesto de excepción al consentimiento previsto en el artículo 27 de la Ley de Protección de Datos Personales, ha generado confusión e incertidumbre, ya que inicialmente dispone que *"en la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento"*. Básicamente en el único caso en que el consentimiento del titular no será requerido es cuando los datos que se obtengan para la confirmación de perfiles puedan ser obtenidos mediante base de datos y documentos accesibles al público.

El Decreto 1558/01 que reglamente la ley 25326 de Protección de Datos Personales establece que: *"Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos*

genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios".-

Ante ello la interpretación que ha hecho la jurisprudencia es que lo que la norma autoriza es la cesión de los datos en cuestión para "la formación de perfiles determinados" que luego resulten útiles para promocionar bienes y servicios. A pesar de la ambivalente frase final de la norma, ello no autoriza a que se transfieran datos sin consentimiento de sus titulares con fines de marketing directo, lo cual –por otra parte- violaría el principio de finalidad antes desarrollado.

Al respecto cabe recordar que en todos los supuestos de tratamiento de datos personales –aun aquellos para los que no se necesita consentimiento del titular de los mismos- es necesario respetar el principio de finalidad para que el tratamiento de los datos sea lícito. La LPDP dispone expresamente que *"Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención"*⁴⁰. La doctrina ha expresado al respecto que *"la legitimidad del fin para*

40 LPDP, art. 4, inc. 3. En concordancia con este principio, el art 11 de la LPDP establece que los datos sólo pueden ser cedidos "para el cumplimiento de los fines directamente relacionados con los intereses legítimos del cedente y cesionario".

el cual el responsable de la base de datos los ha obtenido, es lo que otorga justificación al uso de datos personales de terceros y establece un límite a su utilización".⁴¹ El fallo bajo análisis trata este principio -con relación a los datos de los actores- al referirse a "la información que arroja el usuario en la red cuando ingresa a distintas páginas web y que después será utilizada con una finalidad distinta de la que previó cuando la brindó"⁴².-

El principio de finalidad impide que los datos sean utilizados indiscriminadamente, incluso cuando hayan sido lícitamente recolectados, toda vez que cuando sean utilizados con un propósito diferente, se necesitará un nuevo consentimiento de su titular.

41 CNCom., Sala D, autos "Salvador, Claudio c/ Citibank N.A.", fallo del 22/11/05 (del dictamen de la fiscal de Cámara, que cita la siguiente doctrina: Gozañi, Osvaldo A., "Hábeas data, protección de datos personales", Rubinzal-Culzoni Editores, p. 55; Grimalt Servera, Pedro, "La responsabilidad civil en el tratamiento automatizado de datos personales", 1999, Ed. Comares, p. 193; Murillo, Pablo L., "El Derecho a la autodeterminación informativa", 1990, Ed. Tecnos, p. 142; Álvarez y Cienfuegos Suárez, José M., "La defensa de la intimidad de los ciudadanos y la tecnología informática", 1999, Ed. Aranzadi, p. 31; Carranza Torres, Luis R., "Hábeas data, la protección jurídica de los datos personales", 2001, ps. 61 y 62; Gils Carbó, Alejandra M., "Régimen legal de las bases de datos y hábeas data", 2001, Ed. La Ley, ps. 73 y 74)

42 "Tanús Gustavo Daniel y otro c/ Cosa Carlos Alberto y otro s/ habeas data (art. 43 c.n.)" - Expte. n° 1.791/2003 - Juzgado Civil y Comercial Federal N° 3 de la Capital Federal - Secretaría N° 6 - 07/04/2006

CONCLUSIÓN

En nuestra legislación, contamos con la Ley de Protección de Datos Personales, la cual en el año 2000 colocó a Argentina en la cima de Latinoamérica respecto de la privacidad de datos.

Hoy, con el mundo globalizado, con el avance de la tecnología, las comunicaciones y las fronteras difusas, dicha normativa ha quedado por detrás, no refleja la realidad del derecho viviente ni da respuestas concretas a este mundo real. Es por tal motivo que resulta imperioso encontrar una solución al avasallamiento que están sufriendo los particulares en general sobre su derecho a la intimidad y privacidad, necesitando una protección efectiva de sus datos personales.

La propuesta de cambio normativo, deberá contemplar el consentimiento de otorgar de forma expresa, con términos y condiciones claros; la autodeterminación informativa que cada una de las empresas que se dedican al marketing tecnológico deberán respetar a través de procedimientos sencillos y de fácil acceso para las personas, poniendo en conocimiento a los usuarios que proporcionaron sus datos los que tienen

en su poder, operando de esta forma, el principio de finalidad como una garantía protectoria, ya que si los datos obtenidos para un fin se pretenden utilizar para otro deberá ello ser informado a los causantes.

El tratamiento de los datos personales debe estar pensado para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación a su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, debiendo respetarse las libertades y derechos fundamentales.

Otra circunstancia importancia a establecer en una futura normativa es la autodeterminación informativa que cada una de las empresas que se dedican al marketing tecnológico deberán respetar a través de procedimientos sencillos y de fácil acceso para las personas, poniendo en conocimiento a los usuarios que proporcionaron sus datos los que tienen en su poder, operando de esta forma, el principio de finalidad como una garantía protectoria, ya que si los datos obtenidos para un fin se pretenden utilizar para otro deberá ello ser informado a los causantes. Las políticas de las empresas al recabar el consentimiento deberán estar adecuadas al principio de “privacy by default” y/o “privacy by design”.

La protección de los datos personales configura una impronta real y jurídica, atendiendo a diversas manifestaciones que deben ser tenidas en cuenta a fin de no ver frustradas su tutela y el lugar que ocupa entre los derechos humanos.

Deberán establecerse políticas de privacidad abiertas, claras y concretas, en donde se incluya la educación de los ciudadanos sobre datos personales, como protegerlos y las consecuencias de su cesión.

Finalmente debería esperarse que las empresas dedicadas al marketing tecnológico asuman una responsabilidad proactiva, donde se eduque y forme parte de su política el establecimiento de términos y condiciones entendibles para los usuarios.

BIBLIOGRAFÍA

- Abrutin, Ariel Videoclase “Big Data. Privacy by design y Privacy by default. Autorregulación de las empresas. Internet de las cosas y PDP” recuperable de <https://virtual.flacso.org.ar/mod/book/view.php?id=1191671&chapterid=1436361>
- Bastera, Marcela I., Datos sensibles ¿Es la publicación del dato de afiliación política un dato sensible en los términos

de la ley 25.326?, laleyonline 0003/012953.

- Basterra, Marcela I., El consentimiento del afectado en el proceso de tratamiento de datos personales, laleyonline 0003/010499

- Basterra Marcela I. "Protección de datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales."

- Gozáni, Osvaldo Alfredo *Hábeas Data. Protección de datos personales, Ley 25.326 y reglamentación (decreto 1558/2001)*, Rubinzal-Culzoni Editores, pág. 150 y sgtes

- Granero Horacio R. (2020) *Inteligencia Artificial y Derecho, un reto social*. Editorial Albrematica S.A.

- Halabi, Ernesto (2010) "El derecho a la intimidad y su protección internacional". Extraído del I Congreso Sudamericano de Derecho - 18 de Marzo de 2010. Disponible en: http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00275178149

- Rigaux, François, "La protection de la vie privée..." p. 597, citado por PEYRANO,

Guillermo F. (2002), *Régimen Legal de los Datos Personales y Hábeas Data. Comentario a la ley 25.326 y a la reglamentación aprobada por Dec. 1558/2001*, Lexis Nexis, Depalma, Buenos Aires , p. 250

Normativa

- Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Convenio 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe. Strasbourg, 28.I.1981. Disponible en: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>

- Ley 25326

Fallos

- Salvador, Claudio c/ Citibank N.A., fallo del 22/11/05

- Tanús Gustavo Daniel y otro c/ Cosa Carlos Alberto y otro s/ habeas data (art. 43 c.n.)" - Expte. n° 1.791/2003 - Juzgado Civil y Comercial Federal N° 3 de la Capital Federal - Secretaría N° 6 – 07/04/2006

SISTEMAS DE RECONOCIMIENTO FACIAL, UNA PREOCUPACIÓN PARA LOS DERECHOS HUMANOS⁴³

Lucas Ezequiel Costabel⁴⁴

Mauren Belén Guiretti⁴⁵

Sol Iara Raschkovan⁴⁶

RESUMEN

Actualmente, el reconocimiento facial aparece como una herramienta contemporánea atractiva a los gobiernos que pretenden volver más eficiente la gestión pública. En esa línea, este trabajo se propone realizar un análisis descriptivo sobre esta nueva tecnología, profundizar sobre cuáles son los beneficios y riesgos que implica el uso de la misma, e investigar cuál es el impacto real que tiene para los derechos humanos.

Palabras Clave: *Inteligencia artificial – SRF – legitimidad – gestión pública – privacidad – principio de no discriminación*

43 Enlace al video <https://youtu.be/87Hf3EukLKA>

44 Abogado. Universidad Nacional del Sur, mail de contacto: lucas.costabel@hotmail.com

45 Estudiante. Universidad Nacional del Sur, mail de contacto: mguirettimartinez@outlook.com

46 Estudiante de la carrera de Abogacía . Universidad Nacional del Sur, mail de contacto: solraschkovan@gmail.com

INTRODUCCIÓN

Gracias al desarrollo que ha tenido la inteligencia artificial los últimos años, se ha visto un aumento exponencial en el uso de sistemas de reconocimiento facial (SRF). La posibilidad computacional de almacenar y analizar a altas velocidades grandes cantidades de datos, la sofisticación de algoritmos de aprendizaje automático y el incremento exponencial de la cantidad de datos disponibles en la red, ha generado una transformación radical en el sector tecnológico industrial que promete cambiar la manera en que estamos acostumbrados a relacionarnos con el mundo.

Desde hace unos años esta tecnología está siendo utilizada tanto en el sector privado como público, lo que ha generado un gran debate en torno a dos grandes preguntas: 1) ¿es el reconocimiento facial una tecnología eficaz? y 2) ¿es el reconocimiento facial una tecnología respetuosa de los derechos humanos? Si bien en este caso vamos presentar algunas líneas únicamente referidas a la segunda de las incógnitas, ambas preguntas, de manera conjunta, buscan dar respuesta a un aspecto central, la legitimidad del uso de SRF como método de control de identidad por parte de

compañías privadas y de agentes estatales.

Claro está que ya existen en nuestras sociedades distintos mecanismos de control de identidad, de hecho, siempre han existido sistemas centrados en identificar a las personas, ya sea mediante sus atributos (nombre, número de cuentas bancarias, número de seguridad social), sus datos biográficos (dirección, profesión, educación) y/o sus datos biométricos (fotografías, huellas digitales). Nuestro documento nacional de identidad y nuestra licencia de conducir son claros ejemplos integrados de todos estos elementos identificatorios. (Introna, y Nissenbaum, 2010).

Los SRF, parecería entonces, no deberían originar demasiadas preocupaciones, atento a que solo sería un nuevo mecanismo de control de identidad mediante el uso de datos biométricos. No obstante, el cambio radical que impone el uso de SRF se asienta en que, a diferencia de otros tipos de datos biométricos, las imágenes faciales de una persona, requeridas en esta tecnología, son relativamente fáciles de capturar, no se requiere una distancia estrecha entre la cámara y la persona, y no se requiere una participación activa de

la persona. Los SRF pueden funcionar sin ni siquiera requerir la cooperación, el consentimiento o incluso el conocimiento del individuo (Introna, y Nissenbaum, 2010).

DESARROLLO

Una vez establecida la necesidad de analizar la legitimidad del uso de SRF en nuestras sociedades contemporáneas, debemos profundizar en su definición, diseño y funcionamiento. Un SRF es una tecnología que permite, mediante el uso de inteligencia artificial, la identificación única de un individuo, a partir de la comparación de los modelos biométricos creados del análisis de imágenes faciales (FRA, 2020).

La premisa de la que parten los SRF es que cada persona tiene rasgos exclusivos que permiten su identificación única. Esos rasgos exclusivos son denominados datos biométricos, y pueden ser físicos/fisiológicos (huellas dactilares, reconocimiento del iris, geometría de la mano, etc), o conductuales (reconocimiento de voz, reconocimiento de escritura, etc).

Los SRF, que corresponden al primer grupo, suelen agruparse de manera genérica en una sola categoría, sin

embargo, los SRF refieren a una multitud de tecnologías que pueden realizar distintas tareas con distintos propósitos. Por eso, es importante saber en cada caso particular, si el reconocimiento facial está siendo utilizado para verificar, identificar o categorizar personas (FRA, 2020).

Verificación: La verificación es la comparación uno a uno. En este caso se busca verificar la identidad de una persona al comparar dos modelos biométricos que, se presume, pertenecen al mismo individuo. Los dos modelos biométricos se comparan a fin de determinar si la persona mostrada en las dos imágenes, es o no, la misma persona. Una de las ventajas que posee este sistema es que no requiere que los datos biométricos de las personas sean conservados en una base de datos. Este tipo de tecnología es muy común en los aeropuertos.

Identificación: La identificación es la comparación uno a muchos. En este caso el modelo biométrico de una persona es comparado con los modelos biométricos almacenados en una base de datos (galería), a fin de determinar si la persona se encuentra o no en dicha base. A su vez, la identificación acepta dos modelos:

uno en el cual ya sabemos que la persona que pretendemos identificar se encuentra en la base de datos (Identificación cerrada), y uno en el cuál no lo sabemos (identificación abierta). El uso de sistemas de reconocimiento facial como identificación suele denominarse reconocimiento facial automático, el cual puede realizarse tanto en vivo como de manera diferida.

Categorización: La categorización, a diferencia de las anteriores, busca determinar a partir del reconocimiento del modelo biométrico de la imagen facial, si un individuo pertenece a un grupo social específico. En este caso el reconocimiento facial sirve para extraer información extra sobre una persona, a partir de sus rasgos exclusivos. Este sistema se denomina “análisis facial”, y suele ser usado para la construcción de perfiles. Aunque pueden ser compatibles entre sí, la diferencia con los otros sistemas es importante, ya que en el uso de “análisis facial”, la búsqueda es sobre características compartidas entre grupos sociales, por lo que el sistema no requiere necesariamente la individualización de la persona. Dentro de esta tarea, podríamos incluir también el “reconocimiento de expresiones faciales”.

Como señalamos previamente, en este trabajo vamos a mencionar algunas cuestiones específicas sobre el impacto que los SRF pueden tener sobre los derechos humanos. Esto significa que dejamos para otra ocasión las cuestiones sobre la eficacia de los mismos, relativa a cuestiones técnicas y de desarrollo tecnológico. No obstante, es importante destacar que esta distinción no es menor, por el contrario, debemos asumir que incluso si nos encontráramos frente a SRF plenamente eficaces, donde todas las cuestiones tecnológicas, ambientales y computacionales funcionaran a la perfección, existirían preocupaciones sobre la afectación a los derechos de las personas (Introna, y Nissenbaum, 2010). Aceptando esto, dejaremos de lado en esta ocasión el gravísimo problema de los falsos positivos y negativos que genera la falta de precisión de los sistemas, para centrarnos en aquellas críticas que se hacen desde un paradigma respetuoso de los derechos humanos (FRA, 2020).

Derecho a la privacidad y a la protección de los datos: Estos dos derechos muy vinculados entre sí encuentran una amenaza común en el uso de los SRF, a partir de la captura y almacenamiento de imágenes faciales en bases de datos. La idea de privacidad

cubre un aspecto tanto físico como psicológico, que constituye un aspecto central en la identidad social de las personas. El respeto a estos derechos muchas veces es necesario para el respeto de otros derechos, actuando como pre-requisitos de los derechos a la libertad de culto, conciencia, expresión, etc. Es cierto que es aceptado que estos derechos no son absolutos, pero eso no quita, que, frente a cualquier pretensión de limitarlos, los Estados deben pasar ellos mismos, o garantizar que terceros pasen, un test de legalidad, necesidad y proporcionalidad. Cualquier limitación debe, entonces, cumplir con los siguientes estándares: a) legalidad, equidad y transparencia; b) Propender a un fin legítimo en una sociedad democrática, específico y explícito; y c) cumplir con ciertos requerimientos respecto a los datos utilizados: minimización, precisión, limitación temporal del almacenamiento, seguridad y rendición de cuentas.

Principio de no discriminación: Calificamos a una acción o situación como discriminatoria cuando una persona es tratada desfavorablemente, frente a otra que se encuentra en condiciones iguales y posee características relevantes similares. La discriminación en las decisiones tomadas con base en las

recomendaciones hechas por sistemas de inteligencia artificial suele ocurrir por la existencia de sesgos, los cuales pueden encontrarse tanto en el diseño como en la implementación de los sistemas. Una importante causa de discriminación es la falta de calidad y diversidad en los datos utilizados para entrenar el sistema de inteligencia artificial, lo que suele generar efectos adversos a grupos minoritarios. Es imprescindible romper con la idea de que la tecnología es neutral. Por el contrario, debemos aceptar la intervención humana en el proceso de diseño y de implementación de los SRF. La desigualdad en el trato puede estar justificada, pero sólo si persigue un fin legítimo, y supera el test de necesidad y proporcionalidad.

Derecho a la libertad de expresión, reunión y asociación: El uso de cámaras instaladas en espacios públicos que usan SRF automáticos y en vivo amenaza considerablemente la libertad de expresión, reunión y asociación de las personas. Saber que existe una vigilancia permanente sobre las personas produce un efecto de temor capaz de generar modificaciones voluntarias o involuntarias en el comportamiento de las personas. Este tipo de vigilancia de control desalienta las manifestaciones públicas

atentando contra la participación ciudadana. Frente a esto es necesario que exista una legislación clara donde se limite el poder estatal y privado en el uso de estas tecnologías. Sólo mediante un fin legítimo, específico y explícito, con publicidad sobre el uso de los datos y la ubicación de estos sistemas, con procesos transparentes, con control ciudadano y con rendición de cuentas, es posible la aplicación de SRF automáticos y en vivo que no afecten los derechos humanos de las personas.

CONCLUSIÓN

Existe una preocupación real y razonable sobre los SRF. La legitimidad de estos sistemas depende tanto de la eficacia como del respeto a los derechos humanos. Este breve trabajo pretendió enunciar algunos de los problemas que encuentra ese segundo aspecto de la legitimidad. Como conclusión, podemos afirmar que resulta necesario, tanto para el uso público como privado de estas tecnologías, que exista un marco legal claro, que se pretendan fines legítimos, específicos y explícitos, y que su implementación supere un test serio de necesidad y proporcionalidad. Sólo así será posible el uso de los SRF de manera respetuosa con los derechos humanos y

conforme a los principios democráticos que rigen nuestras sociedades.

BIBLIOGRAFÍA

FRA - European union agency for fundamental rights. (2020). Facial recognition technology: fundamental rights considerations in the context of law enforcement.

Introna, L., y Nissenbaum, H. (2010). Facial recognition technology a survey of policy and implementation issues. *Lancaster University Management School*

LA UTILIZACIÓN DE INTELIGENCIA ARTIFICIAL EN EL DIAGNÓSTICO DE ENFERMEDADES ESPECIAL CONSIDERACIÓN AL CASO DEL COVID-19⁴⁷

Ana V. Visconti⁴⁸

RESUMEN

Esta comunicación considera algunos de los problemas que presentan los sistemas de inteligencia artificial (IA) empleados en el diagnóstico de pacientes y la determinación de sus tratamientos, con una especial consideración al actual contexto de pandemia por Covid-19. La problemática que se plantea surge del contraste entre la falta de transparencia de los procesos algorítmicos empleados por la IA, en su mayoría protegidos por el secreto empresarial, y el derecho a la información que tienen los pacientes de conocer qué factores fueron tomados en cuenta para diagnosticar su patología y decidir la forma de tratamiento.

Palabras claves: Opacidad algorítmica - Salud - Derecho a la información - Covid-19

INTRODUCCIÓN

En el ámbito de la salud los procesos algorítmicos de que se valen los sistemas de IA juegan un rol esencial en el diagnóstico de los pacientes y en la

determinación de sus tratamientos.

Entre los estudios por imágenes diagnósticas, la radiografía de tórax y la tomografía computarizada son los métodos más recomendados ante la

47 Enlace al video https://youtu.be/_FFYNXslrVs

48 Estudiante de abogacía de la Universidad Nacional del Sur; Mail. anavaleriavisconti@gmail.com

sospecha de infección por Covid-19, y su interpretación es determinante en la toma de decisiones clínicas para el manejo de estos pacientes. Con la implementación de softwares de IA, un algoritmo de aprendizaje automático es capaz de detectar, en menos de un minuto, los casos positivos y su gravedad, analizando la radiografía del paciente y comparándola entre cientos de radiografías ya cargadas al sistema.

El empleo de IA en el diagnóstico médico trae consigo grandes ventajas, sobre todo un importante ahorro de esfuerzo y tiempo, a lo que se suma un alto grado de precisión. Sin embargo, la falta de certeza acerca de la transparencia tanto en el funcionamiento como en la calidad de los datos de que se valen los sistemas informáticos, dificulta al profesional médico para cumplir con el derecho a la información de los pacientes previsto en la ley 26.529. Emérito a la brevedad de esta comunicación se mencionarán con la síntesis exigida los aspectos vinculados a la opacidad y al secreto empresarial.

OPACIDAD DE LOS ALGORITMOS

La IA se sirve de procesos algorítmicos para realizar sus predicciones. Existen muchas clases de algoritmos que tienen

distintas aplicaciones en los diversos campos, no obstante, tres son las propiedades básicas que todos ellos presentan, a saber, su universalidad, su opacidad y el impacto que generan en la vida de las personas (Monasterio, 2017). Me centraré en la característica de la opacidad y la repercusión que la misma tiene en la vida, o más concretamente, en la salud de los seres humanos.

Los algoritmos aprenden de los datos con los que se alimentan. Si hay diagnósticos inexactos en la base puede haber predicciones incorrectas en los resultados que arrojen. Por ejemplo, en un estudio del año 2015 liderado por un grupo de expertos estadounidenses, se llevó a cabo un ensayo con el objetivo de determinar la exactitud de una IA para predecir la probabilidad de muerte en pacientes con neumonía. En dicho ensayo, asombrosamente, descubrieron que el padecimiento de asma era calificado por el software como un factor de bajo riesgo de muerte. Debido a que las variables del algoritmo eran visibles, fue fácil explicar el porqué de esta predicción: los pacientes con asma eran inmediatamente enviados a un hospital, con lo cual, el intenso cuidado que recibían reducía su riesgo de muerte tras sufrir una neumonía frente al resto de la población (Caruana et al., 2015).

Imaginemos ahora que en lugar de tratarse de pacientes con neumonía estamos hablando de pacientes con Covid-19. La situación es exactamente la misma y, por lo tanto, no está exenta de presentar errores de diagnóstico. La clasificación hecha por la IA precisa la gravedad del virus en los pacientes y, en base a ello, se determina la necesidad de su internación. Ante una eventual falta de suministros y equipos, el algoritmo podría determinar en los peores escenarios quiénes se beneficiarían con la asignación de respiradores y quiénes no.

En este orden de ideas, podemos observar que los sistemas de IA indican su propuesta, resultado o “decisión”, pero no aportan información significativa sobre en qué elementos o factores causales ha fundamentado aquélla. Cuando las decisiones automatizadas afectan a las personas en su posibilidad de acceder a tratamientos médicos, debe ponderarse el derecho que tienen éstas a una explicación adecuada e inteligible acerca de los datos tomados en cuenta y los procesos llevados a cabo por el sistema para arrojar ese resultado.

Los algoritmos no son objetivos y neutrales como se cree. Ellos se enmarcan siempre en un contexto temporal y espacial influido por el avance

tecnológico y el desarrollo económico y social. Tampoco son independientes de las ideas y creencias de los programadores -o de las empresas por las que son contratados para desarrollar estos sistemas-, muchas veces traducidas en forma de prejuicios, sesgos, estereotipos o intereses empresariales que afectan la imparcialidad de los resultados arrojados por los sistemas de IA (Monasterio, 2017).

SECRETO EMPRESARIAL Y DERECHO A LA INFORMACIÓN DE LOS PACIENTES

Otra cuestión a considerar es que los softwares de IA están protegidos, o bien por las patentes de invención o bien por el secreto empresarial (Azuaje, 2020). Ni los médicos, ni mucho menos los pacientes, tienen acceso a los datos de los que se vale el sistema para llegar a una determinada predicción o de los procesos lógicos utilizados para brindar ese resultado.

Ahora bien, si los médicos desconocen los datos tomados en consideración por la IA para elaborar su predicción, así como la lógica empleada para llegar a ella, carecen de elementos necesarios para dar una explicación fundada relativa al

diagnóstico, su gravedad o la forma de tratamiento propuesta. Con relación a esto evidenciamos que se produce una discordancia entre el derecho a la información del paciente y la protección del secreto empresarial de la que gozan los sistemas informáticos.

En Argentina, el derecho a la información del paciente está previsto en la ley 26.529 y en el art. 59 CCyC. En nuestra legislación se garantiza la libertad de elección y decisión del paciente en el marco de su proceso asistencial, previo conocimiento veraz y comprensible de toda aquella información que sea necesaria para el ejercicio de su autonomía; es decir, el paciente tiene una serie de derechos que debe ver satisfechos.

Para que un profesional médico pueda validar un determinado resultado y tomar una decisión sobre sus pacientes necesita conocer los datos en los que se ha basado la IA para arrojar esa predicción. Como el médico no siempre conoce dichos datos, no estará en posición de cumplir con su deber de informar al paciente en forma clara, suficiente y adecuada.

Además, otro de los problemas que se plantea es el relativo al influjo que ejerce el sistema informático en el médico. Las

decisiones que el galeno toma sinérgicamente con el apoyo de la IA muchas veces pueden verse influidas por el resultado arrojado por el sistema y, como consecuencia, le resulte a aquél muy difícil apartarse de la predicción algorítmica. Es posible afirmar que la capacidad decisoria del médico puede verse contaminada, o cuanto mucho fuertemente condicionada, por el resultado devuelto por el sistema.

Por último, y centrándonos nuevamente en la cuestión del Covid-19, se puede observar que, debido al alto grado de contagio y al desconocimiento sobre la enfermedad, son siempre los médicos del centro asistencial quienes toman la decisión de hospitalizar, brindando escasa información al paciente y su consecuente falta de consentimiento. En este específico supuesto, cabe preguntarse qué posibilidad tienen los pacientes de Covid-19 -o eventualmente sus familiares si es que se produjo el deceso- de exigir acceso a la información en caso de que la elección de un determinado tratamiento - como cuidados ambulatorios- y no otro - como la internación o la derivación a terapia intensiva-, haya sido tomada en base a una predicción propuesta por una IA y el médico no pueda brindar una explicación fundada de tal elección.

COMENTARIO FINAL

Como se ha expuesto, la IA es una herramienta de gran valor para lograr resultados más eficientes y rápidos en el sistema de salud en general. Sin embargo, su empleo implica nuevos desafíos en los que la transparencia es una condición necesaria para lograr soluciones más justas y protectorias de la vida y derechos de los pacientes.

A esta altura de la investigación llevada a cabo por quien suscribe, es posible advertir, al menos, la necesidad de la construcción de un marco jurídico adecuado en el que sea posible garantizar la transparencia algorítmica; se trata de encontrar un equilibrio entre los intereses comerciales de los desarrolladores de IA y los derechos de los pacientes a obtener una información sanitaria completa.

BIBLIOGRAFÍA

- Monasterio Astobiza, A. (2017). Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos. *Dilemata*, 24, 185-217. Recuperado de <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000107/497>
- Caruana, R., Lou, Y., Gehrke, J., Koch,

P., Sturm, M., Elhadad, N. (2015). Intelligible models for HealthCare: predicting pneumonia risk and hospital 30-day readmission [Modelos inteligentes en el servicio de salud: prediciendo el riesgo de neumonía y la readmisión hospitalaria en 30 días]. Recuperado de <http://people.dbmi.columbia.edu/noemie/papers/15kdd.pdf>

- Azuaje Pirela, M. (2020) El dilema de la transparencia algorítmica y los secretos empresariales. Recuperado de <https://adefinitivas.com/adefinitivas-internacional/el-dilema-de-la-transparencia-algoritmica-y-los-secretos-empresariales-a-cargo-de-michelle-azuaje/>.

LA MUTABILIDAD DEL ORDEN PÚBLICO INTERNACIONAL CUANDO CONCURRE CON LA INTELIGENCIA ARTIFICIAL DECISORIA⁴⁹

Corina Andrea Iuale⁵⁰

RESUMEN:

Algunas preguntas surgen cuando se cruzan inteligencia artificial y Orden Público Internacional, preguntas que merecen ser atendidas. Ellas son: ¿La inteligencia artificial puede captar el espíritu de la legislación?, ¿la inteligencia artificial puede llegar a ser considerada como fuente del derecho?, ¿la inteligencia artificial inmoviliza al derecho?, ¿la inteligencia artificial transforma en inmutable al orden público internacional? EL Orden Público internacional resulta ser una defensa, un muro que impide la aplicación del derecho extranjero indicada por la norma de Derecho Internacional Privado. Dicho muro se hace patente cuando el derecho extranjero que debe ser aplicado contradice el espíritu del derecho del Estado. El Orden público internacional es mutable, porque el espíritu de la legislación lo es. Por su parte, la aplicación de sistemas de inteligencia artificial decisoria ¿no conducirían a la petrificación del derecho?.

PALABRAS CLAVE: *Inteligencia Artificial, Mutabilidad, Orden Público, Orden Público Internacional, Derecho Internacional Privado.*

49 Enlace al video https://youtu.be/GjE_1E_ya1s

50 Abogada, Magister en Derecho Privado UNR, Magister en Derecho Internacional Privado UBA, Profesora Derecho Internacional Privado UNS y UNRN ciuale@uns.edu.ar

INTRODUCCIÓN

En la concurrencia del derecho y la Inteligencia artificial, que en adelante será llamada IA, se detecta un problema que refiere al carácter mutable del Orden Público de un Estado. Por su parte, el Orden Público internacional, ocupa un rol central cuando se trata de la aplicación de una norma proveniente de un ordenamiento jurídico de otro Estado.

En el sentido indicado, surgen preguntas que merecen ser atendidas. Ellas son: ¿la inteligencia artificial puede llegar a ser considerada como fuente del derecho?, ¿la inteligencia artificial inmoviliza al derecho?, ¿la inteligencia artificial transforma en inmutable al orden público internacional?

DIVERSOS TIPOS DE SISTEMAS EXPERTOS JURÍDICOS

Entre los dominios de aplicación de la I.A. tenemos los sistemas expertos, la demostración automática, juegos y teoría combinatoria, aprendizaje automático, robótica, procesamiento del lenguaje natural, redes neurales, base de datos

inteligentes, reconocimiento de patrones. Como ven, los dominios de aplicación de la I.A. son muy amplios, cubren muchos aspectos (Munera L. A.).

Un sistema experto es un sistema computacional que puede plantear posibles soluciones a determinados asuntos jurídicos aplicando el conocimiento experto en la materia, así como explicar sus razonamientos (Martinez Bahena, Goretty Carolina Martinez). La autora recientemente citada refiere la existencia de diversos tipos de sistemas expertos jurídicos, tales como los basados en reglas de producción en donde se pretendía transformar la British Nationality Act en una serie de enunciados condicionales formulados de tal forma que si se da tal situación se produce un cierto efecto jurídico; el modelo positivista explícito subyacente en donde se construye un silogismo jurídico con una premisa mayor que consiste en la norma jurídica y una premisa menor en donde se describe el hecho; el modelo constructivista que presenta como principal ventaja frente al modelo positivista que concibe a la norma jurídica no como enunciado explícito contenido en

el cuerpo normativo sino como esquema mental resultante del procesamiento de tales enunciados mediante reglas de razonamiento jurídico que se integran con otros conocimientos con los que cuenta el operador jurídico como son los discursos provenientes de la teoría general del derecho, los provenientes de la argumentación e interpretación, etc. El modelo de razonamiento legal basado en casos en el que se administra una base de casos de los que se infiere el resultado.

Sin perjuicio de la existencia de clasificaciones de sistemas expertos, lo cierto es que resulta inminente que las decisiones tomadas mediante éstos sean utilizadas a fin de emular por completo el razonamiento del juez. Lo expresado indica que en caso que se dé crédito para ello, la inteligencia artificial será admitida con potencial de crear jurisprudencia y en ello como creadora del derecho. Las decisiones, logradas con un muy alto grado de precisión podrían replicarse en otras decisiones del algoritmo en tanto se den las circunstancias previstas para llegar a esa decisión.

Más allá de los grandes datos y de lo valioso que resulta la ausencia de arbitrariedad humana, la decisión lograda según un algoritmo -que es producto de

líneas de programación- no necesariamente recogería las nuevas realidades a las que sí presta atención el juez cuando interpreta al derecho con la finalidad de dictar sentencia.

LA INTELIGENCIA ARTIFICIAL EN LA CREACIÓN DEL DERECHO. EL ORDEN PÚBLICO INTERNACIONAL.

La detección del problema atinente a la relación entre la IA y el Orden Público Internacional se enmarca en el ámbito del Derecho Internacional Privado y la sociedad de la información. Las preguntas formuladas al comienzo de la presente comunicación traen consigo una serie de respuestas que ya tienen los informáticos, pero el análisis de cuyas consecuencias aún resta ser abordadas por los juristas.

La aceptación por parte del ordenamiento jurídico

Ante la cada vez más cercana y efectiva emulación de la decisión del juez, la existencia de esas decisiones generadas por IA muestra la posibilidad de que las mismas puedan ser consideradas como decisiones que se reiteran ante casos análogos. Si bien la presente

comunicación no da espacio para abordar en concreto sobre jurisprudencia como fuente del derecho en el ámbito del Derecho Internacional Privado, se pretende abrir la puerta a esa situación. A lo expresado agréguese algo fundamental y es que la existencia de una IA creadora del derecho será tenida como tal, en la medida que sea aceptado ese carácter por el propio ordenamiento jurídico.

Avanzando en lo previamente expresado en cuanto a la aceptación por parte del ordenamiento jurídico de una IA decisoria con crédito suficiente como para ser considerada creadora del derecho mediante la aplicación de sistemas expertos, la capacidad de aprender que tenga la IA hará que ésta aprenda dentro de su propio lineamiento. Lo expresado es una advertencia que consiste en remarcar que la IA podría decidir sin una necesaria captación de la realidad. Lo expresado indica que debe prestarse atención al riesgo del estancamiento del derecho.

La inteligencia artificial sólo captaría el orden público en su faz estática

Si en el complejo proceso decisorio llevado a cabo mediante IA, se decida en una cuestión de Derecho Internacional Privado -en donde corresponda analizar la aplicación de la ley extranjera-, que dicha

ley vulnera el espíritu de nuestra legislación, dicha decisión será tomada dentro de los límites fijados para el autoaprendizaje de la misma IA. En ese punto, nuevamente aparece el riesgo de estancamiento del derecho, en concreto de su espíritu el que seguramente podrá ser captado solo en su faz estática. Se deduce que si el derecho es dinámico, también lo es su espíritu -orden público- así como su orden público internacional.

Con la finalidad de dotar claridad cabe indicar que orden público es el conjunto de principios que inspiran un ordenamiento jurídico y que reflejan los valores esenciales de una sociedad en un momento dado (Feldstein de Cardenas, Sara, 2017); y que el orden público internacional resulta ser una defensa, un muro que impide la aplicación del derecho extranjero indicada por la norma de Derecho Internacional Privado. Dicho muro se hace patente cuando el derecho extranjero que debe ser aplicado contradice el espíritu del derecho del Estado. El Orden público internacional es mutable, porque el espíritu del derecho lo es.

El artículo 2600 Código Civil y Comercial refiere al mismo cuando establece que las disposiciones de derecho extranjero

aplicables deben ser excluidas cuando conducen a soluciones incompatibles con los principios fundamentales de orden público que inspiran el ordenamiento jurídico argentino.

En Francia, el concepto de orden público internacional tiene una concepción muy parecida a la colombiana, en el sentido que opera como una excepción a la aplicación de una ley o sentencia que vaya en contra de los postulados esenciales del Estado francés (ROLDAN PARDO, 2010).

CONCLUSIONES

En este estadio primigenio de la investigación es posible concluir que se está ante la presencia de una cuestión fáctico-tecnológica, que consiste en prever hasta dónde puede llegar el desarrollo tecnológico; si bien esta cuestión es propia de los informáticos y a las que ya tienen dada muchas respuestas; sí, hay un problema que sí nos alcanza a los juristas, y es el de determinar cuál es el rol que el derecho va a otorgar a las decisiones tomadas a través de inteligencia artificial.

BIBLIOGRAFÍA

- FELDSTEIN DE CÁRDENAS, Sara. Código Civil y Comercial de la Nación y normas complementarias. Análisis doctrinal y jurisprudencia. Comentario art. 2600.
- GORETTY Carolina, MARTINEZ Bahena “La inteligencia artificial y su aplicación al campo del derecho” <https://www.corteidh.or.cr/tablas/r30570.pdf> . Fecha visualización 19-10-20
- MUNERA, Luis Eduardo “Inteligencia artificial y Sistemas expertos” Repository: Universidad Icesi, Colombia: Portal de revistas https://www.icesi.edu.co/revistas/index.php/publicaciones_icesi/article/download/870/870. Fecha visualización 19-10-20
- ROLDÁN PARDO, Juan Felipe “El estado del arte del concepto de orden público internacional en el ámbito del derecho internacional privado y el arbitraje internacional” Revista de Derecho Privado, núm. 44, julio-diciembre, 2010, pp. 1-30 Universidad de Los Andes Bogotá, Colombia

APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO JURÍDICO⁵¹

Carlos Martín Aznar⁵²

RESUMEN

“Inteligencia artificial, aprendizaje profundo, aprendizaje automático... te dediques a lo que te dediques, si no lo comprendes tienes que ponerte con ello y aprender qué es. Porque de lo contrario serás un dinosaurio dentro de 3 años”. Esta frase dicha por un empresario norteamericano Mark Cuban engloba la idea del presente trabajo basada en la disrupción de las tecnologías de la Inteligencia Artificial en el mundo del derecho.

PALABRAS CLAVE: *Machine learning, disrupción tecnológica, inteligencia artificial jurídica.*

51 Enlace al video <https://youtu.be/Ovgq3ERk1GY>

52 Abogado de la UNLP, Especialista en Derecho Tributario Local de la UNTREF. Mail: cmaznar@gmail.com

INTRODUCCIÓN

En el año 1950, Alan Turing proponía una prueba que permitía identificar si una máquina era o no inteligente. Un juez se comunicaría a través de una terminal informática con una entidad en una habitación contigua. Si tras una conversación dicho juez no era capaz de distinguir si con quien se comunicó era o no humana, el ordenador sería considerado inteligente. A raíz de ello, hoy conocemos la prueba de Turing, llamada Completely Automated Public Turing test to tell Computers and Humans Apart - CAPTCHA-, cuando accedemos en la WEB para diferenciar ordenadores de humanos, a fin de evitar que programas automatizados puedan utilizar ciertos servicios o enviar correos masivos.

Años después, Marvin Minsky y John McCarthy le daban nacimiento al campo de estudio basado en lo que llamamos Inteligencia Artificial (IA), estableciendo las bases para crear dispositivos inteligentes.

Luego de un invierno de la IA, empezaron a desarrollarse sistemas inteligentes para actividades específicas, como *Deep Blue* creado por el gigante *IBM* en el año 1996, que fue el primer equipo en ganar una partida de ajedrez contra el Garry

Kasparov, famoso ajedrecista campeón del mundo.

Actualmente, nos rodean agentes artificiales, como los asistentes personales -Cortana, Siri o Google Assistant-, los traductores de idiomas, los chatbots de las empresas u organismos, los filtros de SPAM, el asistente de conducción -Google Maps o Waze-, las recomendaciones de Netflix, de MercadoLibre o de Spotify, el reconocimiento facial del celular, entre tantos ejemplos.

De la misma forma, el ámbito jurídico no quedó exento de esta disrupción tecnológica, creándose múltiples herramientas y aplicaciones que se sirven de los diversos enfoques de la IA, tendientes a concretar tareas que hasta ahora sólo la realizaban las letradas y los letrados.

Está claro que el nuevo desafío es hablar menos en latín y más en binario, es por ello que se desarrollará el avance de estas tecnologías en el ecosistema del derecho.

INTELIGENCIA ARTIFICIAL

De forma muy comprimida y al sólo efecto orientativo podemos brindar algunas

referencias a modo de prelude de la Inteligencia Artificial. Así decimos que, utiliza ordenadores, algoritmos y múltiples técnicas para procesar la información y resolver problemas o tomar decisiones que antes sólo podían ser realizadas por los seres humanos. Así como el cerebro extrae, selecciona, recorta y organiza la información disponible para tomar decisiones, la inteligencia artificial hace lo mismo, pero con otros métodos y a otra velocidad (Bostrom, Nick, "Superinteligencia", Ed. Tell, España, 2016, 2ª ed.)

Dentro de la IA encontramos al *Machine Learning* (ML), en donde se diseñan algoritmos para que la máquina aprenda de la información brindada. El objetivo es crear un modelo que permita resolver una tarea dada, entrenando al mismo usando una gran cantidad de datos. Este modelo aprende de estos datos y es capaz de hacer predicciones o resolver un problema. Es decir, no depende de las reglas del programador sino la máquina por sí sola aprende. Existen varias versiones de aprendizaje automático: el aprendizaje supervisado, el aprendizaje no supervisado y el aprendizaje por refuerzo.

El *Deep Learning* (DL) son plataformas que tratan de imitar el cerebro humano sin

que exista intervención humana previa. Se basan en varias capas de redes neuronales que emulan la forma en que el cerebro humano procesa la información, a través de un gran número de unidades o nodos de procesamiento interconectadas, tal como si fuesen neuronas.

Estos sistemas se utilizan para la traducción automática, el reconocimiento de imágenes y creación de subtítulos, entre tantas otras.

Por último, hay que mencionar al Big Data (BD) como el conjunto de tecnologías, técnicas y herramientas que hacen posible la recogida, procesamiento y análisis de volúmenes masivos de datos y la visualización de los resultados. El propósito es convertir la información hallada en esos grandes e inmensos conjuntos de datos en algo útil como estadísticas, patrones de comportamiento, análisis de rendimiento, etc.

INTELIGENCIA ARTIFICIAL Y DERECHO

Si bien la abogacía es por definición conservadora, en el contexto actual en donde existe un auge de la inteligencia artificial, han surgido una serie de herramientas que prometen generar una disrupción en la actividad jurídica.

(Amunátegui Perelló, Carlos, “Archana Technicae. El Derecho Y La Inteligencia Artificial” Tirant lo blanch Valencia, 2020).

Granero expone con claridad que implementar un expediente digital no consiste —meramente— en digitalizar expedientes; el desafío es cambiar la mentalidad, comprender la importancia de "ser digital", pensar en digital y las cosas que ello facilita y no "pensar analógico", que es volcar a binario lo que hoy está en papel. De lo contrario, si únicamente nos ocupamos de ver cómo despapelizamos, permaneceremos anclados a un concepto de expediente judicial concebido no ya para el siglo pasado, sino más bien para varios siglos atrás (Granero, Horacio R., “AA.VV. - Camps, Carlos E”.., Tratado de derecho procesal electrónico)

Coincide Quadri, que es esencial pensar cómo hacemos para informatizar el proceso y no solamente cómo hacemos para digitalizar el expediente (Quadri, Gabriel H., “Expediente Digital En El Anteproyecto De Reforma Al Código Procesal Civil Y Comercial De La Nación”, Suplemento Derecho, Innovación y Tecnología, febrero 2020)

Tal como los contenidos y la IA de Netflix, Spotify y Google Maps extinguieron a los VHS, los CDs y la guía Filcar, los procesos

y procedimientos digitales deben hacer lo propio con los expedientes papel, los sellos, las cédulas, los formularios papel, los escritos con encabezados, etc.

Juan Corvalán, quien es muy claro con su genial idea de automatizar para humanizar. Dice que si logramos combinar la inteligencia artificial con inteligencia humana y consolidar un paradigma 4.0, se pueden lograr resultados asombrosos que redundarán en beneficios concretos tanto para los ciudadanos como para los trabajadores y funcionarios judiciales. Su idea central no es reemplazar a la persona o desplazarla de su labor, sino que puedan reemplazar tareas mecánicas y rutinarias, para cuestiones que requieran mayor creatividad. Entonces, además de agilizar los procesos, la automatización en el ámbito del derecho, liberará a las personas de realizar tareas rutinarias y mecánicas, para que puedan volcar su potencial intelectual en casos más complejos y retroalimentando la automatización (Corvalán, Juan C., “Inteligencia artificial al servicio de la justicia penal, contravencional y de faltas. “Prometea” en el ámbito de la ciudad de Buenos Aires”. CIBERCRIMEN II. Editorial IBdeF)

En los últimos años se han desarrollado diversas herramientas que rompen con los

patrones clásicos del entorno jurídico, con diversas funcionalidades, algunas que automatizan labores ya existentes y otras que son innovaciones que mejoran el ecosistema legal.

En primer lugar, se resaltan las aplicaciones que utilizan IA para el diseño y confección de documentos. La interfaz elabora, de manera más o menos automática, contratos o *Smart-contracts*, formularios, documentos, modelos de escritos, resoluciones judiciales, actos administrativos, etc. *Rocketlawyer* (<https://www.rocketlawyer.com/> consultado en 2020), *LawGeex* (<https://www.lawgeex.com/>, consultado en el 2020) son algunos de los ejemplos de estas aplicaciones que utilizan árboles de decisión.

Por otro lado, encontramos IA para resolver conflictos de forma automatizada llamada "Online Dispute Resolution" (ODR). *Modria* (<https://www.tylertech.com/products/modria>, consultado en el 2020) es una plataforma que guía a la persona durante el reclamo, brindándole una solución al conflicto planteado. Es usado por *PayPal* y *eBay* para resolver reclamos de usuarios, quienes pueden seleccionar entre varias alternativas, describir su problema y

adjuntar eventualmente la prueba que justifique sus dichos. Se le da traslado al otro usuario y emite automáticamente una posible solución basado en sistemas expertos y redes neuronales. Si alguno de los dos usuarios en conflicto continúa disconforme, se pasa a una segunda instancia en donde interviene una persona humana como mediadora.

Utilizando principalmente las técnicas de ML, encontramos herramientas de análisis de datos en el entorno jurídico. Así, *LexMachina* (<https://lexmachina.com/>, consultado en el 2020) pronostica la probabilidad de que una patente sea aprobada, analizando millones de antecedentes en un poco tiempo. *Ross* (<https://rossintelligence.com/what-is-ai.html>), es capaz de escuchar el lenguaje humano, rastrear diez mil páginas por segundo y formular respuestas para los abogados en un caso determinado. *Blue J Legal* (<https://www.bluejlegal.com/>, consultado en el 2020) identifica patrones en la jurisprudencia en materia fiscal y laboral y efectúa predicciones sobre cómo un tribunal determinado podría resolver un asunto en función de los parámetros ingresados por el usuario.

A su vez, en el sector público y en el privado, hallamos chatbots jurídicos. *Chat*

with Billy (<http://www.billybot.co.uk/>, consultado en el 2020), es un buen modelo de chat multiplataforma que incorpora motor de búsqueda.

En el ámbito nacional, *PROMETEA* (<https://ialab.com.ar/prometea/>, consultado en el 2020), combina detección inteligente, predicción, asistencia inteligente y automatización. Agiliza y optimiza exponencialmente procesos burocráticos para mejorar los derechos de la ciudadanía. Posee un sistema de pantalla única e integrada, para combinar automatización de diversas tareas, asistencia digital para obtener información relevante y, por último, elabora documentos de forma íntegra, que también pueden ser producto de una predicción.

En el fuero penal, Estados Unidos utiliza más de 5.300 aplicaciones desarrolladas con estas tecnologías, incluyendo drones con control a distancia, cámaras con ALDPR (*Automated License Plate Reader*) que leen y registran los datos de las patentes de los automotores, su ubicación, hora y fecha generando una base de datos y mapa de circulación, cámaras con reconocimiento facial, sistema de detección de disparos, mapas criminales o *hot spots*. *The Predictive Policing* (www.predpol.com, consultado en el 2020)

es de capaz de predecir cuáles son las zonas más problemáticas en una ciudad determinada.

Ahora bien, también es dable resaltar que esta oportunidad de entrar en la “cuarta revolución” en el campo jurídico, necesita de marcos regulatorios innovadores y adaptados, sin los cuales resulta complicada su instrumentación.

CONCLUSIÓN

La clave es dejar de pensar al proceso judicial o administrativo como un expediente, como un íter, una secuencia de documentos, individual, autónomo. Es el primer paso ineludible para incorporar luego estas herramientas en auge que ayudarán a mejorar la labor jurídica, optimizarla y automatizarla.

BIBLIOGRAFIA

- Technicae. El Derecho Y La Inteligencia Artificial” Tirant lo blanch Valencia, 2020
- Bostrom, Nick, "Superinteligencia", Ed. Tell, España, 2016, 2a ed.
- Granero, Horacio R., "AA.VV. - Camps, Carlos E"., Tratado de derecho procesal electrónico.

- Quadri, Gabriel H., “Expediente Digital En El Anteproyecto De Reforma Al Código Procesal Civil y Comercial De La Nación”, Suplemento Derecho, Innovación y Tecnología
- Corvalán, Juan C., “Inteligencia artificial al servicio de la justicia penal, contravencional y de faltas. “Prometea” en el ámbito de la ciudad de Buenos Aires”. CIBERCRIMEN II. -<https://lexmachina.com/>
- <http://www.billybot.co.uk/>
- <https://www.tylertech.com/products/modria>
- <https://www.bluejlegal.com/>

RESPONSABILIDAD PENAL DEL PROGRAMADOR Y LA EMPRESA DE INTELIGENCIA ARTIFICIAL⁵³

Nicolás Mario Grandi⁵⁴

RESUMEN:

Los software de inteligencia artificial se presentan como innovadores para el campo de derecho penal y resulta complejo encontrar un campo dogmático con el abordarlos. Existen múltiples diferencias entre estos sistemas autónomos y los productos tradicionales, como por ejemplo la independencia de sus acciones, su inmaterialidad, su categoría ontológica, etc.; sin perjuicio de ello la responsabilidad por el producto podría ser una forma adecuada al momento de tener que valorar la responsabilidad criminal tanto del programador como de la empresa tecnológica. Sin embargo, esta dogmática penal no es de aplicación automática, sino que debe ponderarse como ha sido los algoritmos entrenados éticamente para saber si sus acciones pueden ser abarcadas por el riesgo permitido.

Palabras claves: responsabilidad penal por el producto; posición de garante; ética de la inteligencia artificial; previsibilidad.

53 Enlace al video: https://youtu.be/3kKBb_3Kn6M

54 Abogado, Docente e investigador. Facultad de Periodismo y Comunicación Social UNLP. Mail: drgrandinicolos@hotmail.com.

INTRODUCCIÓN

La responsabilidad penal por el producto no surge de la creación ilícita de un riesgo sino el mero hecho de que el productor, en la búsqueda de intereses económicos, legalmente crea un riesgo para el público en general al liberar un producto cuyas reacciones no puede predecir con seguridad y control, incumpliendo así su deber objetivo de cuidado.

Este deber, que coloca en una posición de garante respecto de su producto, está dado por las diferentes artes técnicas y legislaciones que le dicen al fabricante como debe llevar adelante un producto seguro, con el fin de hacer previsible su uso y consecuencias de éste.

Esto que funciona con los productos tradicionales, es una cuestión que entiendo que debe analizarse en el campo de la Inteligencia Artificial (en adelante IA) dado que ésta presenta múltiples diferencias con sus antecesores.

DIFERENCIAS ENTRE LA IA Y LOS PRODUCTOS CONVENCIONALES

La primera gran diferencia que presenta la IA respecto de los productos tradicionales es que esta ha sido creada con el fin de actuar con independencia de su usuario o creador, lo cual le da una cierta

imprevisibilidad a sus actos.

Esta condición única, lleva a la necesidad de que esas acciones independientes puedan ser luego analizadas con el fin de asignar responsabilidad.

Por ello, tanto la Organización de las Naciones Unidas (ONU, 2020, puntos 36 a 38) como la Unión Europea (European Commission, 2019), han realizado documentos tendientes a dar parámetros para generar IA confiables sobre la base de la explicabilidad y transparencia de sus actos.

Allí, expusieron que todas las acciones de los sistemas inteligentes deben ser trazables, explicables y comunicables, en tanto, en el supuesto de encontrarnos ante un sistema de IA de caja negra, se debe propiciar otras medidas de explicabilidad (por ejemplo, trazabilidad, auditabilidad y puede ser necesaria una comunicación transparente sobre las capacidades del sistema, siempre que el sistema en su conjunto respete derechos fundamentales).

Otra diferencia importante entre la IA y los productos convencionales, es que a los software inteligentes las personas les asignan una categoría ontológica, lo cual implica que si bien no los ven como seres vivos, tampoco los consideran como un mero objeto, en síntesis los aprecian

como algo completamente nuevo que está entre ellos y los objetos (Khan, 2011); lo cual nunca había ocurrido, con otro tipo de producto.

Otra cuestión diferenciadora de la IA es su inmaterialidad, justamente nos encontramos ante algo que no tiene un elemento corpóreo determinado, sino que, lo que hace es usar un soporte material para poder desarrollarse.

Recién podríamos tener alguna similitud con los otros productos cuando la IA se inserta dentro de un hardware y allí adquiere corporalidad pero, como producto en sí, su base es la inmaterialidad.

Justamente en esta interacción, entre hardware y software se genera otro de los elementos complejos a la hora de valorar la responsabilidad penal de los productos con IA, el cual es la multiplicidad de actores que interviene en su desarrollo e implementación.

Los algoritmos pueden ser concebidos en términos de múltiples capas de hardware, protocolo y software que ofrecen múltiples oportunidades para la innovación pero, esta gran cantidad de participantes, a contraposición, podría dificultar el establecimiento responsabilidad ante un comportamiento que es perjudicial (Balkin, 2015).

Asimismo, estos sistemas tienen la capacidad de absorber datos de distintas fuentes y en diferentes etapas de su desarrollo e implementación, y si éstos son erróneos o sesgados pueden condicionar la toma de decisiones.

Muchas veces se habla de los sesgos algorítmicos, en los cuales, la máquina analiza datos y termina tomando una determinación de manera discriminatoria.

Ya la Unión Europea ha puesto el foco sobre esta cuestión y ha dicho que el sesgo identificable y discriminatorio debe ser eliminado en la fase de recolección cuando sea posible (European Commission, 2019, punto 1,5).

Otra cuestión vinculada con la inmaterialidad es que la IA debe ser programada sobre la base de una ética, dado que la ética práctica de una red neuronal no se halla en su arquitectura, sino que reside en la función error que empleamos para entrenarla y la importancia de ello, está siendo reconocida en el mundo entero⁵⁵.

55 La función error o también llamada "*utility function*", tiene el deber de mostrarle al algoritmo la cantidad de errores que comete cada vez que realiza una acción, cuanto más errores cometa peor será si desempeña, en tanto que cuanto menos, mejor hará su trabajo. En sí, la función error le dice a la máquina que debe aprender. Justamente la función error es el corazón del problema en donde se decide qué tipo de IA estamos construyendo.

Múltiples organismos se han pronunciado sobre esta cuestión y han dado una serie de parámetros en los cuales se debe sustentar éticamente la programación de la IA (Asilomar, 2017; ONU, 2020, puntos 27 y 28; European Commission, 2019; US Association for Computing Machinery, 2017).

Allí se expuso que la IA debe respetar y considerar, enumera la dignidad humana, los derechos humanos y las libertades fundamentales, no dejar a nadie atrás, vivir en armonía, fiabilidad, transparencia, trazabilidad, auditabilidad, verificación, protección del medio ambiente y supervisión humana.

Esta apreciación sobre los elementos éticos que deban tener las máquinas es relevante para el campo penal, pues, a mi criterio, marcarán el rumbo de lo que será el riesgo permitido sobre la base de la previsibilidad.

CONCLUSIÓN

De lo expuesto hasta aquí se puede observar que existen varias diferencias entre la IA y los productos convencionales, sin embargo hay una que destaca sobre el resto.

Esta es su autonomía en la toma de decisiones, lo cual da una cierta imprevisibilidad respecto a cómo va a

proceder ante eventos no programados.

Justamente, la cuestión de la autonomía y la imprevisibilidad es lo que divide las aguas en cuanto a la responsabilidad penal de los creadores sobre las acciones de sus obras.

Por un lado, tenemos aquellos que sostienen que al ser autónoma, el programador no será responsable por lo que haga (Hellstrom, 2013, p. 99. 107), y por el otro aquellos que pregonan que, sin perjuicio de su actuar independiente su creador debe responder por las acciones que lleva adelante por cuestiones de responsabilidad profesional (Nagenborg, Capurro, Weber y Pingel, 2013, p. 349/366).

Sin embargo, no creo que la discusión en cuanto a la responsabilidad penal por las acciones llevadas por una IA deba centrarse en su autonomía pues ello limitaría las posibilidades de que los programadores y las empresas se animen a ir por más, en busca de mejorar la IA y brindar mejores servicios a la sociedad.

A mi modo de ver, la cuestión debe ser enfocada principalmente en cómo los programadores y las empresas tienen en cuenta los diferentes preceptos éticos dados por los diversos organismos tanto públicos como privados a la hora de desarrollar y llevar adelante sus

proyectos.

Parto de esta posición pues entiendo que la programación ética es la única que permitirá dar una cierta previsibilidad a las acciones autónomas llevadas adelante por la IA ya que dejará saber con antelación sobre la base de qué elementos, la máquina tomará sus determinaciones.

Como se explicó al comienzo de este artículo, la responsabilidad del fabricante surge del incumplimiento de las diferentes artes técnicas y legislaciones que le dicen al productor cómo debe llevar adelante un producto seguro, con el fin de hacer previsible su uso y sus consecuencias, lo cual permite que estas quedan abarcadas dentro del riesgo permitido⁵⁶ y, en consecuencia, exento de sanción penal.

Los riesgos de poner una IA a interactuar son muy altos, dado que es difícil saber cómo procederá en distintas circunstancias, máxime cuando su accionar depende de la información que

⁵⁶ Este riesgo puede ser entendido como un peligro generado por los hombres y presentarse como la conceptualización jurídica del precio que la colectividad debe pagar para disfrutar de los beneficios del progreso. Si bien, la creación de riesgo es un sinónimo de puesta en peligro, no toda puesta en peligro de un bien jurídico es merecedora de una pena pues la creación consciente de éste puede parecer aceptable, cuando las consecuencias positivas ligadas a eso superan claramente a las consecuencias negativas. Así, en esta ponderación de costos y beneficios reside la idea básica de la figura del riesgo permitido.

se le suministra por fuera de su programación, si creamos una IA cuyo fin es desarrollarse y evolucionar.

Esto podría llevar a que, si se valora únicamente la autonomía como eximente de responsabilidad, todas las acciones criminales llevadas autónomamente por una IA quedarían exentas de sanción. En tanto, si nos paramos de la otra vereda y entendemos que la independencia de la máquina no exime de responsabilidad, todas las acciones dañinas de la IA harían responsables a sus creadores, sin perjuicio de que ellos no hicieron nada para que eso ocurra.

De esta manera, nos encontraríamos ante el problema de: por un lado dejar que la IA actúe sin responsabilidad, lo cual no resulta aconsejable, o por el otro castigar a su creador sin perjuicio de que éste realizó la IA con fines loables y las acciones del software nunca pudieron ser controladas.

Al pensar como se diseña un sistema de responsabilidad penal para la IA, no podemos perder de vista los fines sociales y comerciales que tiene esta tecnología. Por ejemplo, se prevé que el uso de Vehículos Autónomos reducirá en un 90% los accidentes viales, reducirá el tiempo de viaje, bajará las emisiones de gases y ruidos. También se estipula que los robots

podrán acompañar a las personas mayores, y brindar asistencia en caso de ser necesario, mejorar ámbitos laborales, entre muchos otros usos supuestos (Oppenheimer, 2018).

Entonces se debe idear un modelo que no limite la innovación en este campo, con la sombra de la posible responsabilidad constante ni, por el otro, deje un libre albedrío en el cual se permita crear IA sin importar las consecuencias que traerá, dado que nadie será responsable.

En una dinámica entre la ética en la programación y la responsabilidad penal por el producto entiendo que está el punto medio correcto en la actualidad.

BIBLIOGRAFÍA:

- Asilomar IA Principles, (2017), Recuperado el 13/8/20 de: <https://futureoflife.org/ai-principles/> .
- Balkin, Jak M., (2015) 'The Path of Robotics Law,' California Law Review Circuit, Vol. 6.
- European Commission , (2019) "Ethics Guidelines for Trustworthy AI", B-1049. Bruselas
- Hellstrom, T. (2013). On the moral responsibility of military robots. Ethics and Information Technology, 12(2), 99–107.
- Khan Peter H, and other, (2011). "The

New Ontological Category Hypothesis in Human-Robot Interaction", Recuperado el 10/8/20 de <https://dl.acm.org/doi/10.1145/1957656.1957710>

- Nagenborg, M., Capurro, R., Weber, J., & Pingel, C. (2008). Ethical regulations on robotics in Europe. AI & Society, 22(3), 349–366.
- Oppenheimer, Andrés (2018) "Sálvese quien pueda. El futuro del trabajo en la era de la automatización" Edit. Debate.
- Organización de las Naciones Unidas, (2020) "Primera versión del proyecto de recomendaciones sobre la ética de la Inteligencia Artificial" SHS/BIO/AHEG-AI/2020/4, París
- US Association for Computing Machinery (2017) "Statement on Algorithmic Transparency and Accountability". Recuperado el 13/8/20 de http://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

CONSIDERACIONES SOBRE LA ASIGNACIÓN DE RESPONSABILIDAD PENAL A LA INTELIGENCIA ARTIFICIAL⁵⁷

Federico Daniel Arrué⁵⁸

RESUMEN:

El trabajo procura ordenar algunas ideas sobre la hipotética asignación de responsabilidad penal a sistemas de inteligencia artificial en cuanto a argumentos a favor de su establecimiento, compatibilidad con las distintas teorías de la finalidad de la pena e implicancias para el paradigma penal del ser humano como único sujeto penalmente responsable.

Se encuadra en una invitación a un debate serio y continuo sobre la asimilación de la inteligencia artificial a los seres humanos en las distintas áreas del derecho.

Palabras Clave: Inteligencia artificial – Responsabilidad penal- Reproche penal – Pena – Teorías de la pena.

INTRODUCCIÓN Y ESQUEMA DEL TRABAJO

Desde estas acotadísimas líneas procuraremos ordenar algunas ideas sobre las posibles ventajas de asignar responsabilidad penal a sistemas de inteligencia artificial y las dificultades que

esto conllevaría.

Primeramente daremos cuenta de posibles argumentos a favor del establecimiento de tal responsabilidad. En segundo lugar, referiremos a su viabilidad desde el punto de vista de la finalidad de la pena. Seguidamente resaltaremos que

57 Enlace al video <https://youtu.be/7JogBIUPVJs>

58 Abogado, Especialista en Derecho Penal. Magister en Derecho. Investigador y Docente de las cátedras de Filosofía del Derecho y de Ciencia Política en la Universidad Nacional del Sur. federicoarrue@hotmail.com

el paradigma clásico del derecho penal que consagra al ser humano como único sujeto penalmente responsable ya ha sido roto en el derecho argentino, por lo cual la hipotética irrupción de la responsabilidad penal de la inteligencia artificial sería menos abrupta de lo que puede pensarse en un primer momento. Por último, cerraremos con unas palabras finales.

Por razones de espacio no haremos referencia a qué puede entenderse por inteligencia artificial ni a la compatibilidad de las penas previstas en el Código Penal argentino con ella, ni tampoco a posibles nuevas penas que pueden llegar a establecerse específicamente para sancionar a una inteligencia artificial.

ARGUMENTOS A FAVOR DEL ESTABLECIMIENTO DE LA RESPONSABILIDAD PENAL DE LA INTELIGENCIA ARTIFICIAL.

Nuevo incentivo a los productores.

Para la creación de inteligencias artificiales que guarden el máximo nivel de seguridad, los productores tienen diversos incentivos tales como evitar su posible propia responsabilidad por no haber realizado los controles necesarios al producto antes de su puesta en el mercado o por no haber tomado las

medidas necesarias si la falla surgiera con posterioridad. E, incluso libres de responsabilidad penal –si actuaron con total diligencia-, es esperable también que procuren que ninguna inteligencia artificial que lleve su firma se vea envuelta en un hecho dañoso que le sea a ésta reprochable.

En este sentido, la eventual responsabilidad penal de la inteligencia artificial podría conllevar que los productores realicen un seguimiento aún más exhaustivo a fin de evitar la publicidad negativa superlativa que implicaría que uno de sus productos fuera condenado penalmente.

Extensión de las posibilidades de actuación del sistema penal.

El establecimiento de la responsabilidad penal de la inteligencia artificial implicaría también que, en los hechos dañosos donde ésta esté involucrada como sujeto activo de un presunto delito, tome intervención –de oficio, en la mayoría de los casos, según el Código Penal argentino- el órgano Fiscal. En sus manos estaría, en primer término, el esclarecimiento de lo ocurrido y la determinación de una eventual responsabilidad penal, como paso previo al juzgamiento en tal sede. De no ser así,

la determinación judicial de los hechos dañosos estaría librada a la existencia de una acción civil por parte de la víctima, puesto que la Fiscalía sólo intervendría de resultar plausible la responsabilidad penal del productor de la inteligencia artificial, de un tercero que ilegítimamente haya alterado a ésta o del usuario humano.

La consagración de la responsabilidad penal en cabeza de la inteligencia artificial, entonces, en determinados casos puede habilitar las posibilidades de actuación de la justicia penal.

Facilitación de la acción civil.

Equiparación de situaciones.

La intervención del sistema penal en casos donde no existe una persona física imputada tiene también un beneficio ligado a la compensación económica por el daño causado. Esto es así porque -dejando de lado el problema de la concreta ejecución de una condena penal sobre una inteligencia artificial-, su sola existencia es relevante, no sólo por su rol simbólico social sino porque facilita el ejercicio de una eventual acción civil por parte de la víctima o sus familiares. Basta pensar en la práctica habitual del fuero penal, donde muchas veces el interés principal del damnificado en la condena pasa por ver reforzadas sus eventuales

aspiraciones económicas dado que, frente a un veredicto de culpabilidad, en sede civil ya no puede discutirse hecho ni autoría.

En este sentido, la víctima de un hecho producido por una inteligencia artificial puede verse en una desventaja procesal en relación a la víctima de un hecho similar provocado por una persona física.

Mantenimiento de la confianza en el sistema penal.

Por último, diremos que en una presuntamente no tan lejana sociedad donde la inteligencia artificial pasaría a realizar una cantidad variada y substancial de actividades cotidianas, su responsabilidad penal puede ser conveniente para la reafirmación de la vigencia y eficacia del sistema. Es decir que, al ser el comportamiento y funciones de las inteligencias artificiales cada vez más semejantes al de los seres humanos, su inimputabilidad resquebrajaría la confianza ciudadana en las normas prohibitivas y punitivas de conductas. Así, para parte de la población, podría tornarse complejo entender y aceptar que una inteligencia que realiza habitualmente las mismas conductas que un humano no sea juzgada penalmente por un hecho que, de ser cometido por un humano, conduciría

sin dudas a su procesamiento.

El ciudadano podría concebir, de modo más o menos consciente, a las inteligencias artificiales como entidades que *optan* por delinquir –pese a que no esté claro que pueda ser sin más expresado de ese modo- y que, pese a eso, si no fuera reputada penalmente responsable, quedaría impune.

Esta función punitiva simbólica no podría ser reemplazada por medidas de prevención administrativas, pues éstas operan por fuera de lo penal.

LOS PROPÓSITOS DE LA PENA A LA INTELIGENCIA ARTIFICIAL DESDE LAS DISTINTAS TEORÍAS

La *concepción retributiva de la pena* entiende que es justo o correcto que el delincuente reciba un castigo en atención a su acto, independientemente de cualquier debate sobre la utilidad o beneficio social o personal de éste. Desde esta perspectiva, corresponde punir a la inteligencia artificial si puede considerársela moralmente responsable, lo cual presumiblemente esté ligado a que haya desarrollado la capacidad de comprender –en un sentido semejante al humano- las nociones básicas de bien y de mal, y, además, que haya desarrollado

también la capacidad de receptor sentimientos no deseados, dolorosos – también en un sentido similar al humano- asociados a la pena. Es decir, que esta línea de pensamiento sobre la función de la pena tendrá sentido si la inteligencia artificial puede, de alguna forma, concebir el mal: tanto el que ha realizado como el que habría de recibir en justa retribución.

En contrapartida, las cuatro teorías de la función de la sanción llamadas *preventivas* se centran en atender a la utilidad ésta.

La finalidad de *prevención especial negativa* de la pena implica que ésta debe aplicarse para neutralizar la potencialidad delictiva del delincuente concreto que la sufre. Esto sería plenamente aplicable a la inteligencia artificial en cuanto ésta pase a no poder o tener dificultada la comisión de nuevos delitos mientras dure la sanción que se le haya impuesto.

La finalidad de *prevención general negativa* considera que la pena debe imponerse para desalentar al conjunto de potenciales delincuentes de cometer hechos delictivos. La pena es vista como un ejemplo atemorizante.

Entendemos que esta visión también resulta aplicable a la punición de la inteligencia artificial, la cual puede servir para amedrentar a personas físicas. El

mensaje de amenaza del sistema penal a la sociedad será de una entidad tal que ni siquiera algunos programas informáticos estarán al margen de él.

Por otra parte, incluso es posible que la sanción impuesta a una inteligencia artificial pueda influir en el comportamiento de otra inteligencia artificial, si esta pudiera receptar el dato y tenerlo en cuenta para su propio accionar.

La finalidad de *prevención especial positiva* plantea que el castigo puede servir para que el delincuente que lo sufre recapacite sobre su conducta y no reincida en el delito. Es la teoría de la rehabilitación y la reinserción social. Trasladado a la inteligencia artificial, en línea con lo que se dijo anteriormente, tendría sentido siempre cuando el programa tuviera la capacidad de internalizar la sanción que él ha sufrido como un dato de la realidad que modifique a futuro sus cálculos con miras a minimizar la posibilidad de que su curso de acción escogido sea un delito.

Por último, en cuanto a la finalidad de *prevención general positiva*, ésta se basa en que la sanción reafirma ante la sociedad la vigencia y efectividad tanto de la norma penal violada en la comisión de delito como del sistema penal en general. Tiene un papel pedagógico, comunicativo

y demostrativo de la superación de un conflicto jurídico.

Creemos aplicable lo dicho en cuanto a la prevención general negativa. Desde esta óptica tendría sentido punir a la inteligencia artificial en tanto muestra –a las personas físicas y eventualmente también a otras inteligencias artificiales- el correcto funcionamiento de la normativa y del sistema penal.

EVOLUCIÓN SOCIAL Y CAMBIOS DE PARADIGMA

Pretender la responsabilidad penal de la inteligencia artificial conlleva problemáticas que pasan no sólo por la justificación teleológica de la imposición de una sanción penal (tal como se ha apuntado), sino también por el amoldamiento de dichas sanciones a las características propias de los nuevos sujetos punibles (a lo que, tal como anticipamos, no referiremos aquí). A esto se suma la posible ruptura de las concepciones de acción y de culpabilidad –dentro de la teoría estratificada del delito- que aporta la dogmática penal, ligadas a la persona humana como único sujeto penalmente responsable.

En relación a esto último, sin embargo, el cambio ya ha comenzado, puesto que en

el derecho argentino, actualmente, las personas físicas no son los únicos sujetos susceptibles de responsabilidad penal y las penas previstas en el Código Penal no son las únicas sanciones del sistema punitivo. Esto es así desde que la ley 27.401, del año 2017, complementaria del Código Penal, establece la *responsabilidad penal aplicable a las personas jurídicas privadas* por determinados delitos.

La responsabilidad penal de personas jurídicas –y, por analogía, de inteligencias artificiales- no carece tampoco de sustento doctrinario, ya que las *concepciones funcionalistas del Derecho Penal*, al no reconocer límites ónticos, entienden que la opción de sancionar penalmente es pura decisión legal.

Como en esta perspectiva los conceptos jurídicos del Derecho Penal no pueden ser independientes de los fines político criminales –y políticos, en general- del sistema penal, es el legislador quien, a partir de dichos fines, decidirá quién es penalmente sancionable. Así, del mismo modo en que la evolución de la sociedad llevó a establecer la conveniencia de la responsabilidad penal de las personas jurídicas, adaptando la normativa penal a sus especificidades; puede también llegar a evaluar la conveniencia de pautar la responsabilidad penal de la inteligencia

artificial, con las adaptaciones que ello requiera.

PALABRAS FINALES

Creemos que, a medida que las inteligencias artificiales cobran relevancia en nuestra vida cotidiana y en nuestra sociedad, corresponde dar paso a un debate serio y continuo sobre su asimilación a los seres humanos, en las distintas áreas del derecho, incluido el ámbito penal. Dicho debate, académico, técnico y legislativo, debe estar abierto a la posibilidad de grandes cambios de paradigmas, semejantes a los que las nuevas tecnologías están imprimiendo ya en nuestra cotidianeidad.

BIBLIOGRAFÍA

- Anitua, Gabriel Ignacio (2002), Historia de los pensamientos criminológicos, Buenos Aires, Editores del Puerto.
- Granero, Horacio R. (Director académico) (2020), Inteligencia Artificial y Derecho, un reto social, Buenos Aires, Albremática.
- Raffo, Francisca Emilia, Nuevas tecnologías y derecho penal (2019), La responsabilidad penal de la inteligencia artificial.

<http://repositorio.udesa.edu.ar/jspui/handle/10908/16303> .

- Zaffaroni, Raúl Eugenio (2018), Manual de Derecho Penal – Parte General, Buenos Aires, Ediar.

Segunda Parte

Presentación: Digitalización y Derecho Procesal Electrónico

Reflexiones sobre la importancia del eje del encuentro y sus discusiones

Prof. Abog. José María Lezcano

El segundo eje del encuentro giró en torno al modo en que se introducen nuevos elementos de Tecnologías Digitales (TD) en las Instituciones Jurídicas, haciendo especial foco en aquellas de carácter procesal. Tales elementos o componentes de TD se incorporan a las administraciones de Justicia e Instituciones con bajo una perspectiva racional-legal. Sus objetivos son, resolver problemas comunes a todo tipo de organizaciones, así como aquellos que son propios de la labor de los operadores jurídicos en el ejercicio de la abogacía, de la judicatura, entre otros.

Bajo una mirada sistémica, en el sistema de la Administración de Justicia es posible encontrar diferentes tipos de elementos: aquellos componentes de carácter normativos (códigos, acordadas, normas en general), aquellos referidos al capital humano (empleado/as, funcionario/as, jueces/zas y todo los vínculos organizativos entre ellos), aquellos que podríamos definir como componente simbólicos (prestigio, jerarquías, aspectos políticos, de argumentación), así como también aquellos de carácter tecnológicos. En estos últimos, es posible considerarlos tanto en software como en hardware, y

las posibles articulaciones e innovaciones que ofrece el mercado: plataformas de redes sociales, aplicaciones de pago, de comunicación, así como de infraestructura, móviles, monitores, dispositivos periféricos, scanner, etc.

A partir de esta distinción elaborada en términos explicativos, las comunicaciones presentadas en este eje, marcaron planteos sobre la manera en que los componentes de TD, no sólo se incorporan al derecho, se enlazan, se aplican, sino que van generando una profunda transformación cada uno de los demás elementos del propio sistema general que lo contiene. Ello, con una característica particular de esta relación, la cual se encuentra en la alta y variada interacción entre sistemas abiertos, como es el caso de los sistemas sociales, culturales, jurídicos, económicos, etc. con sistemas cerrados y de puntuales intercambios con el entorno, como ocurre con los sistemas informáticos.

En esta segunda parte se ordenan los artículos función de una continuidad

temática que da cuenta de los temas de interés y preocupación en el ámbito académico. Preocupación que, a partir de la simplicidad que ofrecen ciertos conceptos jurídicos fundamentales, se aborda la complejidad y profundidad del cambio que enfrenta el derecho y el mundo jurídico.

Sobre algunas discusiones teóricas y empíricas, se reproducen debates necesarios sobre el posicionamiento epistémico y político. En particular, sobre los horizontes y escenarios abiertos en la relación del Derecho y la Tecnología. Así, en este apartado se focaliza en uno de los ámbitos bien funcionales y fuertemente instrumentales de la ciencias jurídicas: el Derecho Procesal y la administración del servicio de Justicia.

Desde estos lugares comunes, se discuten problemas jurídicos, algunos de los cuales encierran paradojas verse forzada su integración con las estructuras e instituciones jurídicas. Muestra de esto ocurre al discutir la recursividad de las decisiones judiciales, cuando estas (las decisiones judiciales), son tomadas en

base a la IA. ¿Qué criterios o parámetros podrían utilizarse para considerar que una IA es superior a otra? ¿cómo se encuentran las personas y operadores jurídicos, frente a la posibilidad de abrir la instancia recursiva?

De este modo, ante la pregunta ¿la IA se debe considerar en las decisiones o en el análisis de las circunstancias que facilita la función al juez?, es posible discutir sobre su “*aletheia algorítmica*”, poder conminatorio y estrechez “ética” que discute Éric Sadín(2020), al analizar el poder enunciativo de la verdad que la IA propone. Desde ahí, los debates en torno a los planteos procesales sobre pertinencia, validez, apariencia de verdad, entre otros, impactan fuertemente en los aspectos sustanciales del acceso a los derechos en su totalidad.

¿Cuáles son los ámbitos, espacios y modos en los que se puede aplicar la IA dentro del proceso?. Es que, como se plantea en algunos aportes, al utilizarse para probar hechos del caso a través de algoritmos, presenta el

problema de conocer cuál es el camino lógico por el cual se llega al resultado. Entonces, se construyen interrogantes cómo ¿se cumple el deber de motivación del juez en la sentencia? ¿se puede reemplazar el sentir del juez o la sana crítica a través de IA?

En los debates y los aportes que venían del eje anterior, como en los de este propio eje, se puede considerar que una de varias de las características de estas TD, la opacidad, la falta de auditabilidad y la confianza en los criterios de expertos tienen significativos efectos en los derechos fundamentales de los destinatarios del servicio de justicia.

Partiendo desde una posición en la que se reconoce la *no neutralidad* de las tecnologías (bajo la diversidad de argumentos y contraposiciones a esto) y más allá de las discusiones éticas, ideológicas e incluso técnicas, pero se impone preguntarnos: ¿qué pasa con los Estados cuando genera políticas públicas que involucran el uso y aplicación de IA? ¿cuales son los análisis, planes y expectativas del

sector público en la incorporación de tecnologías, cuando en su mayor parte es desarrollada por el sector privado?

Ante el camino que alerta Fernando Barrio de una sociedad que parece ir desde una utopía hacia una distopía, es imprescindible los estudios sobre el “para qué”, el “cómo” y qué objetivos institucionales y políticos se persiguen con la incorporación de estas tecnologías digitales. Para ello es necesario pensar cómo se genera la política pública que luego se transforma en derecho. Cabe considerar que la política pública (también no neutral) debe hacerse desde la multi y la interdisciplinariedad, por lo que es fundamental ampliar los escasos estudios previos y posteriores a la incorporación de tecnología en la sociedad y las instituciones, con un análisis crítico y desde los derechos humanos.

Es que el tono de las discusiones sobre estos temas, llevan a los debates sobre el control, el castigo y la vigilancia en una sociedad panóptica.

Sociedad e instituciones en la que las decisiones se apoyan en parámetros determinados por desarrolladores y programadores cuyos sesgos (de su propia humanidad) se encuentran presentes también en sus algoritmos y programas.

Programas y sistemas que en la relación de derecho y tecnologías digitales, construyen relaciones y fenómenos socio jurídicos, que en gran medida denotan características de ubicuidad, reticularidad, convergencia tecnológica, instantaneidad, entre otras, que son propiedades emergentes de la complejidad que involucra.

En los capítulos 3ro. y 4to. que componen el apartado se encontrarán artículos aportados por docentes, investigadore/as, estudiantes (vario/as de ellos ya graduado/as) y profesionales de la abogacía que discuten sobre estas líneas. Les invitamos a recorrer estas páginas y observar las presentaciones en el canal del encuentro



Capítulo 3

Algunos enunciados sobre las Tecnologías Digitales en el Proceso Judicial



TECNOLOGÍAS DIGITALES Y PROCESO JUDICIAL. UNA COMPLEJA RELACIÓN ENTRE INSTRUMENTOS Y PRINCIPIOS⁵⁹

José María Lezcano⁶⁰

RESUMEN

Como punto de partida, es importante considerar que la relación entre tecnologías digitales y normas en la Sociedad de la Información (SI), siempre ha sido asimétrica. Al enfrentar la interpretación de fenómenos socio-técnicos, en particular procesales, nos encontramos con el problema de reconocer cuál es el sentido y orientación que van conduciendo los diversos modos de integrar las Tecnologías Digitales (TD) en el sistema jurídico procesal. A partir de marcos teóricos sobre la filosofía de la tecnología, es posible reconocer al menos tres perspectivas teóricas que explican, interpretan y consideran la aplicación de los aspectos propios de relación tecnología-sociedad, en particular en el ámbito del Derecho Procesal Electrónico (DPE).

En este aporte, se realiza una interpretación del problema que nace del avance tecnológico frente al modo el cual el derecho y las prácticas sociales se integran en un proceso de apropiación y significación. Para ello, sintéticamente se describen los puntos fundamentales de las perspectivas en las que se enmarca la relación tecnología y sociedad, para considerar la integración de los llamados principios del DPE en la dimensión del derecho informático, en el Derecho Procesal y en la aplicación de estos por los operadores del servicio de justicia.

PALABRAS CLAVES: *cambio social – instrumentalidad – teorías de la tecnología – apropiación/significación – uso/consumo .*

59 Enlace al video <https://youtu.be/ZYFJyQSmWyA>

60 Abogado. Docente-Investigador GECSI-FCJyS-UNLP. mail: josemlezcano@gmail.com

INTRODUCCIÓN

La relación entre tecnologías digitales (TD) y normas formales, siempre ha sido claramente asimétrica. Lo cual es fácilmente comprensible si partimos de la lógica jurídica de que no todas las conductas posibles pueden ser contenidas de manera exhaustiva en el texto, sean estas leyes, acordadas, disposiciones, etc. La estructura jurídica kelseniana organiza una solución jurídica, reglamentada. Siendo las distintas conductas posibles mediatizadas por las tecnologías, el esquema formal/reglamentario, desde una perspectiva de inflación legislativa, aumenta la complejidad del sistema (Olivera, 2009).

Por su parte, el modo en que las tecnologías digitales (tanto en software como hardware) han transformado las prácticas sociales, depende de diversos factores: nivel de desarrollo, brecha digital, resistencias al cambio, entre otros.

Hemos planteado en diferentes ámbitos (Gerlero, Lezcano y Liceda 2019; Lezcano, 2019a y 2019b), una distinción que realiza Feenberg (2008) sobre las corrientes filosóficas y sociológicas respecto de la tecnología. En esta línea, la perspectiva que se adopte en relación al vínculo Sociedad y Tecnología, afecta

claramente a las consideraciones que hagamos sobre el llamado “Derecho Informático” y por supuesto también sobre el considerado Derecho Procesal Electrónico.

En las próximas páginas, se presenta una breve distinción de estas ideas, trayendo aspectos puntuales que a mi juicio ilustran una mejor comprensión de ellas, para culminar en un modo pretendidamente propositivo sobre el tema.

EL PROBLEMA: LAS TENSIONES EN EL PROCESO DE CAMBIO

La significación de los principios procesales, desarrollada tanto por la doctrina, la jurisprudencia y la academia, han ido adquiriendo sentidos que buscan contextualizar la estructura de la resolución de conflictos judiciales a las aplicaciones posibles que las tecnologías digitales permiten. Esta viabilidad o posibilidad que las TD ofrecen, varias veces tensionan tanto con estructuras e instituciones jurídico-procesales, como con aspectos que resultan intrínsecos a la evolución misma de los grandes sistemas tecnológicos (Hughes, 1987).

Por mencionar un ejemplo de estos efectos, los aspectos de “notificaciones judiciales” dentro del proceso, viene recorriendo un interesante derrotero tanto

a nivel nacional⁶¹, como en la provincia de Buenos Aires⁶², Neuquén, Mendoza, Córdoba⁶³, por mencionar algunas⁶⁴. Hoy, las posibilidades de notificación mediante actuales sistemas de mensajería instantánea, no sólo tensionan con las interpretaciones de la notificación

61 El antecedente “Bravo Ruiz, Paulo César c. Martocq, Sebastián Marcelo y otros s/ daños y perjuicios” (2016) de la CSJN indica que cuando se constata una consecuencia grave y disvaliosa (dejar desierto un recurso por la omisión de acompañar copias digitalizadas), procede dejar sin efecto las actuaciones previas para dar plena vigencia al derecho de defensa en el marco de una litis judicial. Ello manifiesta la tensión que produce el cambio tecnológico con las garantías constitucionales y del proceso.

62 Por mencionar un significativo ejemplo, los autos “Herrera, Ricardo Horacio y otro/a contra Herrera, María Aurora. Desalojo” –Causa C. 121.320- SCBA marca, entre otras cosas, un interesante punto de referencia en la materia, pero además ilustra un interesante recorrido del proceso de apropiación/significación de los sistemas y agentes que intervienen.

63 Puede encontrarse un interesante estudio comparativo y propositivo de algunas jurisdicciones locales en “Robledo, Diego; La notificación electrónica en Argentina. A propósito de la implementación de las nuevas tecnologías en el proceso judicial.” (2014) En el trabajo, el autor indica que es necesario atender a la capacitación, difusión y educación de los usuarios y potenciales usuarios, en un diálogo democrático con los prestadores del servicio, los operadores jurídicos, abogados y abogadas, y la sociedad para informar públicamente sobre este cambio y modernización del sistema. Propone un necesario “registro y medición de la calidad del sistema, que ofrezca una autoevaluación institucional, pero también un control del foro de abogados y de la sociedad, para propiciar mejoras con el transcurso del tiempo”.

64 Las recientes Ac. 3989 de creación del “Registro de Domicilios Electrónicos del Poder Judicial de la Provincia de Buenos Aires” y Ac. 3991, que incorpora los artículos 11 y 12 al “Reglamento para la notificación por medios electrónicos”, establece las “notificaciones automatizadas” como una forma válida para comunicar las decisiones del/la Juez/a en los casos que corresponda.

procesal⁶⁵ y la defensa en juicio (entre otros), sino también con aquellos aspectos que las TD nos traen, sobre todo en nuestros países, como brecha digital⁶⁶, seguridad informática⁶⁷, entre otras.

En este orden de ideas, el pretendido expediente digital o electrónico, representa tanto una oportunidad como un doble riesgo. La primera, en el sentido de diseñar un proceso de resolución de un conflicto judicial que resulte contemporáneo al contexto social, cultural y tecnológico de la Sociedad de la información. El doble riesgo lo encontramos en las fronteras entre el proceso tradicional escaneado -por un

65 Explicaba el maestro Couture que “la palabra “notificación” en el lenguaje forense, representa, indistintamente, el acto de hacer saber la decisión, el acto de extender la diligencia por escrito y el documento que registra toda esa actividad.” (Fundamentos de Derecho Procesal Civil, pág. 205)

66 Siguiendo a Kemly Camacho (2006), en reiterados trabajos hemos asumido el concepto de brecha digital como una manifestación de las demás brechas sociales, pero que en el mundo de las TD se pueden considerar en un triple sentido: 1) el enfoque hacia la infraestructura: o sea, la posibilidad/dificultad de disponer de computadoras conectadas a la red mundial; 2) el enfoque hacia la capacitación: es decir, la capacidad/dificultad de usar estas tecnologías; 3) el enfoque hacia el uso de los recursos: se refiere a la limitación/posibilidad que tienen las personas para utilizar los recursos disponibles en la red. Este último, muchas veces no identificado, es fundamental pues apunta hacia la igualdad de oportunidades.

67 Es importante plantear 3 planos de seguridad: la informática, que nace del plano de las ciencias informáticas y sus problemáticas; la tecnológica, en la que además de la informática, también se incorpora el factor o intervención humana; y la jurídica, que como operadores jurídicos conocemos su sentido, y desde hace ya algunos años, en el contexto de TD adquiere una significación

lado- y que el proceso sea conducido por aquellas posibilidades y potencialidades del desarrollo tecnológico, en los que el sistema informático determina una lógica propia que se impone al sistema judicial y procesal.

Por ello, la decisión de las Cortes (nacionales y locales), así como los/las jueces/zas que deben decidir no solo sobre el fondo, sino también sobre la forma en que se llevan a cabo los procesos, necesitan diseñar y construir un sistema jurisdiccional que evolucione de acuerdo al desarrollo socio-técnico (Thomas, 2008), no sólo en un contexto de pandemia global, sino en una sociedad de la información (SI) y una cultura digital que inicia la tercera década del siglo XXI⁶⁸.

68 En este orden de ideas, puede encontrarse una relación reconfigurada de las notificaciones en base al principio de la ubicuidad. Es decir Palacios explica que las notificaciones son los actos mediante los cuales se pone en conocimiento de las partes, o de terceros, el contenido de una resolución judicial. En cuanto a las formas, Arazi indica que es un elemento de todo acto procesal (junto al sujeto y al objeto) y materializa la forma en que se exteriorizan los actos procesales. Ellas además de expresar cómo se celebra el acto, involucra también el tiempo y el lugar, el dónde y cuándo debe desarrollarse el acto de notificación. Entonces, podemos encontrar ese vínculo directo entre la localización territorial, del la lógica en que se constituyó esa figura, con la ubicuidad de las TD, en primer término otros aspectos claves como la inmediatez, sincronía/asincronía, entre otros.

LA TECNOLOGÍA DESDE LA FILOSOFÍA Y LAS CIENCIAS SOCIALES

Desde una perspectiva filosófica y sociológica de la técnica y tecnología, Feenberg (1991), sistematiza y describe tres teorías que plantean posiciones respecto del análisis social de la tecnología: la Teoría Instrumental, la Teoría Sustantiva y la Teoría Crítica de la tecnología. Esta distinción sobre el modo de considerar las TIC nos permite, por un lado 1) reconocer la existencia de más de un marco explicativo sobre la tecnología, y 2) admitir que cada uno de estos puntos de vista lleva a proyecciones socioculturales, económicas y jurídicas diferentes, con gran impacto la hora de aplicar e interpretar la relación entre tecnología y sociedad. Las primeras dos posiciones, han sido dominantes en la consideración político filosófica de la sociedad capitalista, en tanto que la tercera, emerge a partir del cuestionamiento a aquellas y la reflexión sobre algunas categorías y conceptos en los que se fundamentan. Así, plantea una teoría crítica de la Tecnología que permite abordar el análisis poniendo el acento en el proceso de *apropiación y significación* de las TIC.

Las Teorías Instrumentales son las que tienen una mirada más dominante. En

ellas la tecnología es considerada neutral, sin contenido valorativo propio, en tanto que es pura "instrumentalidad", es indiferente de la variedad de fines para los que pueda ser utilizada⁶⁹. De manera que el enfoque instrumental es identificado como una manera de ver al hombre y la máquina, en donde el primero es influido por ella en su vida profesional, en el caso de abogado/as y jueces/zas, campo de las prácticas y actos jurídico-procesales. Pero se trata de una manera de ver que permite tener presente que la técnica es la que engloba a los dos y que la máquina no es más que una expresión de aquella. Es además, una forma de considerar que la tecnología empieza y termina en la máquina⁷⁰. La imagen instrumental separa a los objetos tecnológicos de su entramado social de manera que bajo esta perspectiva, se podría considerar que las tecnologías son productos neutros, siendo la sociedad la responsable de su uso, ya que, en principio, la tecnología no

69 Dice Feenberg: "Se basa en la idea del sentido común de que la tecnología son 'herramientas' que están listas para servir a los propósitos de los usuarios. La tecnología está considerada 'neutral' sin un contenido valorativo propio." ("Teoría Crítica de la Tecnología. Introducción: el Parlamento de las cosas. Tecnología y el fin de la Historia", pág. 2)

70 Al considerar únicamente la fase artefactual de la tecnología y asumir su carácter neutral, se corre el peligro de convertir a los expertos, científicos e ingenieros, en aquellos que detentan el poder de decidir lo que es tecnológicamente "correcto y objetivo", dejando por fuera la participación de la comunidad en toda decisión tecnológica.

respondería más que a los criterios de utilidad y eficacia, desvinculado de factores políticos o sociales.

Las teorías sustantivas, se caracterizan por el determinismo. En ellas, lo técnico es una fuerza cultural autónoma capaz de arrasar todos los valores tradicionales con los que compite. Esto significa que su mera utilización trae consecuencias para el hombre y la naturaleza que trasciende el logro de objetivos meramente técnicos. Es así que la ética y valores propios que las TD están plasmados en la sociedad, nacen desde el propio diseño de las tecnologías. Sedimentadas en las prácticas cotidianas, su diseño inspira el uso y consumo, que por momentos parece adquirir carácter de imprescindible para la vida social.

Finalmente, las teorías críticas, se encuentran en la intersección entre la ideología y la técnica, en donde las dos se aprecian para controlar a la sociedad y a los recursos, en conformidad con los llamados "códigos técnicos", los cuales, de manera invisible sedimentan valores e intereses en reglas y procedimientos, instrumentos y artefactos que rutinizan la búsqueda de poder y ventajas por una hegemonía dominante. En este sentido, se presenta una relación dialéctica que se manifiesta en la praxis, bajo la cual la tecnología no es una cosa, sino un

proceso ambivalente de desarrollo que se distingue de la neutralidad, debido al rol que le atribuye a los valores sociales en y desde el diseño mismo de la tecnología.

Una de las consecuencias más destacadas estas ideas, es dejar de considerar el vínculo uso/consumo de la tecnología por parte de los individuos, para centrar la mirada en un proceso de apropiación/significación en la relación tecnología y sociedad.

LOS LLAMADOS PRINCIPIOS DEL DERECHO PROCESAL ELECTRÓNICO

En los últimos 15 o 20 años se vienen analizando la configuración que tienen los principios procesales a partir de la incorporación de TD en el desarrollo del proceso y la actividad jurisdiccional. Un referenciado trabajo de De Resende Chaves Júnior (2012) propone una enumeración y desarrollo de principios de específicos del Derecho Procesal Electrónico.

De manera muy sintética, estos se mencionan como 1) el principio de la inmaterialidad, referido a la digitalización, la transformación del contenido a través del lenguaje de bit, propio de las máquinas; 2) el principio de la conexión (tanto reticular como inquisitiva) tanto desde el punto de vista tecnológico, como

también social y procesal⁷¹; 3) el principio de intermedialidad, que no sólo involucra los contenidos “planos”, sino también otros tipos de contenidos como imágenes y sonido; 4) el principio de la hiperrealidad, por el cual en un medio electrónico, se puede registrar una realidad digitalizada, codificada y virtualizada (hiperrealizada); 5) el principio de la interacción, que expresa del principio contradictorio, pero en un ámbito digital permite otras dimensiones de este. Busca superar la expresión clásica de la contradicción lineal, segmentada y estática, por un contradictorio más intenso, instantáneo, con una transformación cualitativa; 6) el principio de la instantaneidad, dado la celeridad propia de las TD, se vuelve más dinámico el proceso, buscando superar lo secuencial, hacia una idea de flujo - workflow- del proceso, no necesariamente

⁷¹ Este principio dentro del proceso, va en línea al que llamamos “de reticularidad” en el ámbito del análisis socio-jurídico del derecho y la tecnología. La red está en la lógica misma de las relaciones que se pueden establecer entre los agentes. No obstante lo cual, esta reticularidad es diversa y depende del tipo, nivel y estructura de red que se construya (centralizada, descentralizado o dispersa). La matriz interconectada desde y por diversos puntos limitan las lógicas lineales y causalidades simples, presentando una multicausalidad y efectos expansivos en diferentes direcciones. Lezcano, J.M. “Sitios de Redes Sociales: Aportes para su análisis a través de un marco teórico sociojurídico”. Simposio de Informática y Derecho – JAIIO 2019. y Lezcano, J.M.: “La emergencia del plano político en el análisis de las plataformas de redes sociales”. En el XX Cong. Nacional y X Latinoamericano de Sociología Jurídica. SASJu. UNLaPam. (2019)

lineal, sino conducido a partir de eventos procesales; y 7) la deslocalización, que busca superar la concepción física de territorio hacia una fluidez efectiva de derechos. Esto es en línea a la ubicuidad que es propia de muchos aspectos de las TD.

Es esta línea de ideas, el autor propone que los operadores del proceso tengan capacidad de aprender errores y la ineficiencia del proceso tradicional, aprovechando la oportunidad de catalizar lo que llama externalidades de red, en beneficio de la efectividad social de los derechos.

Lo que se percibe es que el proceso electrónico transita en otro orden, distinto de la tradición de la escritura, pues traduce la combinación de lo inmaterial que es lo electrónico, con lo reticular propio de las TD. Es muy importante considerar que según el autor, el proceso electrónico tiene potencial de ser mucho más que la infraestructura de TD en el proceso tradicional, sino que transforman radicalmente la naturaleza del proceso tradicional, caracterizado primordialmente por la separación de los “autos” del mundo. El proceso electrónico es, sobre todo, proceso en red.

Sin embargo, cabe preguntarse, bajo qué perspectiva o teorías de la tecnología es

considerada la incorporación de inteligencia artificial en el expediente, en los nuevos modelos de gestión judicial, en las consideraciones sobre la prueba, en las audiencias virtualizadas y tantas otras transformaciones que van ocurriendo en el proceso. ¿Será instrumental o sustantiva? ¿cuál será la interpretación que le darán los/as jueces/zas a las formas y a los contenidos? ¿cuál será la perspectiva de los supremos Tribunales de Justicia?

Es posible pensar que en este esquema, los principios tradicionales del derecho procesal adquieran nuevas dimensiones e interpretaciones. No estamos experimentando sólo un cambio en el soporte del principio escriturario, sino en la dinámica misma de la comunicación, en el principio dispositivo de las partes, en el principio de contradicción, en el principio de la publicidad, en la economía procesal, en las dinámicas, seguridad y percepción de las pruebas, entre otros.

Por su parte, la cultura tribunalicia genera prácticas diferenciadas y propias, que muchas veces corren en paralelo con la realidad formal. A partir de nuevas dinámicas de comunicación, de datos, la gestión judicial y las interacciones de los actores del sistemas se reconfiguran. Estas alcanzan otras dimensiones, con grandes potencialidades para mejorar la

calidad y eficacia de servicio de justicia, pero también con importantes riesgos de exclusión y vulneración de derechos fundamentales.

A MODO DE CIERRE

Es entonces que, para lograr quizás la humanización del proceso judicial que propone Ávila Paz (2005), en la que invita a buscar la eficacia sin desmedro de las garantías y alcanzar la tutela judicial de la persona y su dignidad, se nos presenta la necesidad de reconocer cuál es la perspectiva o mirada que se le está dando a la relación entre tecnología y sociedad. Es pensar un Poder Judicial a escala humana como explica Alberto Binder⁷².

En esta línea, es necesario considerar que las tecnologías no son el fin en sí mismo, sino el medio para articular un mecanismo de resolución de conflictos en una sociedad que presenta características de disgregada y compleja (Gerlero, 2018). Por ello, la significación de los principios procesales, van adquiriendo sentidos que buscan contextualizar la estructura de un proceso en un contexto de potencialidades pero también riesgos.

72 Conferencia Magistral del Dr. Alberto Binder "Por un Poder Judicial a Escala Humana", en el cierre del 3er. Congreso Nacional de Derecho de la UNLaPam. Disponible en https://www.youtube.com/watch?v=D_3lzopHa-M (9 de Octubre de 2020)

Por ello, el modo en que se considere a la tecnología en el desarrollo de este proceso, está determinado por una tensión entre al menos dos ópticas sobre las TD que es conveniente identificarlas, así como ver cómo actúan y sus consecuencias en la estructura misma del proceso. Por ello, considero que es necesario focalizar el análisis a partir de una perspectiva crítica de la tecnología, en un proceso de apropiación y significación de las TD aplicadas al proceso judicial, que permita alcanzar de mejor manera un mecanismo judicial de resolución de conflictos acorde a los efectos y circunstancias de la sociedad actual.

BIBLIOGRAFÍA

- Camps, Carlos E., "Principio dispositivo y el Código Civil y Comercial de la Nación", La Ley, 01/02/17, cita online: AR/DOC/4999/2016
- Camps, Carlos E. (Dir.) "Tratado de Derecho Procesal Electrónico" (VVAA). Ed. Abeledo-Perrot, Bs.As., Argentina (2016)
- De Resende Chavez Junior José Eduardo de Resende Chaves Júnior; "El Expediente en Red y La Nueva Teoría General del Proceso"; Biblioteca Digital Gratuita de E-Justicia Latinoamérica; [en línea]; <http://wp.me/p4n5ZR-6n> ;
- Feenberg, A. "Teoría Crítica de la Tecnología. Introducción: El parlamento de las cosas. La tecnología y el Fin de la

Historia”. en *Critical Theory of Technology*, Oxford University Press, 1991. Traducción de Miguel Banet, (2000). Disponible en https://www.sfu.ca/~andrewf/books/Spain_El_Parlamento_de_las_Cosas.pdf

- Feenberg, A. “Teoría crítica de la tecnología”. *Revista CTS*, no 5, vol. 2, Junio de 2005 (pág. 109-123). Traducción de Claudio Alfaraz (revisión de Diego Lawler).

- Gerlero, Mario S. “Introducción a la Sociología Jurídica”; Ed. David Grinberg, Bs. As., Argentina (2006)

- Gerlero, M. S. “Haciendo Sociología Jurídica”. *Visión Jurídica Editores*, Bs. As. Argentina. (2018)

- Lezcano, J. M. “La Emergencia del Plano Político en el Análisis de las Plataformas de Redes Sociales”, en el XX Congreso Nacional y X Latinoamericano de Sociología Jurídica. SASJu – UNLPam. Santa Rosa, La Pampa, Argentina (2019)

- Lezcano, J. M. y Liceda, E. “Anotaciones de inicio para un diagnóstico situacional de la digitalización del poder judicial de la Provincia de Buenos Aires” en el 2das. Jornada de Investigaciones Socio-Jurídicas. Instituto de Cultura Jurídica, FJCyS-UNLP, La Plata, Argentina (2018).

- Olivera, N.: “Estado de la cuestión en la relación entre derecho e informática”. *ANALES de la FCJyS Nro. 40.*, La Plata, Bs. As. Argentina, disponible en <http://sedici.unlp.edu.ar/handle/10915/21016>

- Robledo, Diego; La notificación electrónica en Argentina. A propósito de la implementación de las nuevas tecnologías en el proceso judicial; Universidad Autónoma de Asunción; *Revista Juridica*; 2; 1; 5-2014; 47-55.

Disponible en <http://revistacientifica.uaa.edu.py/index.php/juridica/article/view/210>

- Thomas H., Buch A. “Actos, Actores y Artefactos. Sociología de la tecnología” Ed. UNQ, Quilmes, Bs.As. Argentina (2013)

LA TRANSFORMACIÓN DEL PROCESO JUDICIAL: DEL IUDEX A LA INTELIGENCIA ARTIFICIAL⁷³

Andrés S., Díaz Etulain⁷⁴ y Javier M., Yabante⁷⁵

RESUMEN

Nuestra propuesta es presentar a la inteligencia artificial como una herramienta para agilizar el proceso judicial, imprimirle mayor celeridad y otorgarle mayor objetividad a las sentencias, a partir de su desarrollo en tres etapas progresivas y acumulativas. Estas etapas son: automatización de partes del proceso, asistencia de la inteligencia artificial al juez y posibilidad del dictado de resoluciones por la inteligencia artificial.

PALABRAS CLAVES: Inteligencia artificial, proceso judicial, objetividad, celeridad.

INTRODUCCIÓN

Basta con consultar a cualquier ciudadano argentino, para dar cuenta, que la sociedad percibe como excesivos los

plazos judiciales, la existencia de sobrecarga de trabajo en los tribunales y la existencia de muchas resoluciones carentes de objetividad o mejor dicho,

73 Enlace al video <https://youtu.be/MU2Zt8HjODc> (Título modificado para la publicación)

74 Estudiante de la carrera de Abogacía de la Universidad Nacional del Sur y miembro del PGI “Análisis económico de los derechos de protección del consumidor”, Mail de contacto: xagodiaz@gmail.com .

75 Estudiante de la carrera de Abogacía de la Universidad Nacional del Sur. Mail de contacto: javierjujui@gmail.com .

viciadas de rasgos de subjetividad humana.

Este trabajo se enfoca en presentar la inteligencia artificial y su implementación en el proceso, mediante tres etapas progresivas, como una manera de hacerle frente a estas cuestiones. Y así, permitir un acabado cumplimiento de principios constitucionales tales como: la tutela judicial efectiva y el plazo razonable; y los principios procesales de celeridad y objetividad por parte del juez.

APROXIMACIÓN AL CONCEPTO DE INTELIGENCIA ARTIFICIAL

Antes de comenzar a delinear como será la evolución de la inteligencia artificial en el proceso judicial, entendemos necesario detallar el concepto que aplicaremos de inteligencia artificial.

En efecto: es aquel sistema informático, que funciona, con mayor o menor grado, en base a dos principios: "Autonomía" y "adaptabilidad". Con ellos desenvuelve una "conducta" o "comportamiento" específico que podemos considerar como "Inteligente", siendo innecesario para su desenvolvimiento, "que comprenda" lo que hace, o "entienda" su entorno al efectuarlo. De ello se desprende su

naturaleza artificial: que cuenta con una función específica y que desenvuelve un comportamiento objetivo. Es decir, la acción que realiza es carente de cualquier tipo de atribución moral, entendimiento o comprensión del acto.

ETAPAS DEL DESARROLLO DE LA INTELIGENCIA ARTIFICIAL

a. partes del proceso.

El primer momento estará dado por la modificación en la forma de realizar los diferentes actos procesales. Pasando de ser manuales a ser realizados de manera automática, mediante el uso de software que así lo permita.

En el marco de esta etapa, Gabriela F. Gil⁷⁶, destaca que podría aplicarse para los diferentes actos procesales, la clásica lógica "if-then-else" (que se traduce en "Si sucede tal cosa, haga esto; si no, haga esto otro"). En este caso concreto, por ejemplo, ante la presentación de la demanda con los requisitos exigidos por el artículo 330 del CPCCN, automáticamente un programa podría

76 GIL, Gabriela F., "La inteligencia predictiva como herramienta de eficacia en la gestión judicial", SJA 21/11/2018, 21/11/2018, 35, (documento digital, AR/DOC/3637/2018, p. 5).

disponer el traslado, o en cambio, si no los cumple, tal programa procedería a su rechazo.

Un elemento esencial que apoya este avance está dado por el decreto de “Tramitación digital, remota, simple, automática e instantánea”, N° 733/18 del Ministerio de Modernización de la Nación. Así, el artículo 10, invita a todos los poderes de las diferentes provincias a: *“impulsar acciones...que permitan la tramitación digital completa, remota, simple, automática e instantánea de todos los trámites que se realicen en la República Argentina”⁷⁷.*

Algunos de los actos procesales que pueden ser automatizados son: los proveídos, la confección de oficios, la acumulación procesos, resoluciones de caducidad, certificación del período probatorio⁷⁸.

b. Asistencia de la inteligencia artificial al juez

La segunda etapa se caracterizará por el hecho de que la IA asiste en la sentencia

77Decreto 733/18, disponible en Infoleg:<http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/313243/norma.htm>.

78GIL, *op. cit.*, (documento digital, AR/DOC/3637/2018, pp. 7-9).

al juez. En efecto, la IA, mediante el análisis de las pruebas ofrecidas, detalles del caso, de la normativa, principios jurídicos básicos, etc., daría una sentencia que el juez deberá seguir obligatoriamente. Ello será así, dado la objetividad de la misma, esto ofrecerá una sentencia carente de carga emocional, afectiva y moral. La misma deberá sentenciar principalmente en función de tales pruebas.

Destáquese que la IA llegaría a dicha sentencia a través de actos de mensura de la prueba, probabilísticas, etc. No entiende el entorno de lo que analiza, se limita a realizar su función, que no es otra que dar una sentencia objetiva. En este sentido no podría dar un fundamento en palabras, y menos en sentido jurídico, de cómo llegó a esa sentencia. Por esta razón, la tarea del juez será complementar esa actividad de la IA, dándole un fundamento jurídico conforme a esa sentencia objetiva dada por la IA. En efecto, la IA indicará cual será la sentencia y el juez redactará los fundamentos de dicho fallo.

c. resolutorias por la inteligencia artificial

Creemos que luego de muchos años, llegaría la tercera etapa. En ella se vería

la culminación del deseo primero del derecho. Aquello que hemos representado físicamente a la “Justicia”: una mujer con los ojos tapados, una balanza en una mano y la espada en otra. Estamos hablando de la verdadera objetividad.

En esta etapa encontramos que la IA ya es capaz de traducir la probabilística que le permite llegar a una sentencia, en palabras humanas y jurídicas. Es decir, puede dar fundamento de ello, emancipándose del juez.

Dichas resoluciones gozarán de un aspecto realmente objetivo, libre de sesgos subjetivos que posee la persona humana (la propia personalidad, la existencia de prejuicios, experiencias personales vividas, la posibilidad de ser corrompido, los intereses económicos, la afiliación a una determinada afiliación política o ideológica, sus valores, estado emocional del momento, la religión que profesa, etc.).

Tal como surge de lo expuesto, entendemos que estamos en presencia de una evolución progresiva. A medida que se vayan sucediendo las diferentes etapas, la inteligencia artificial aportará al proceso, cada vez una mayor objetividad

y celeridad, logrando finalmente ser el reemplazo idóneo del juez.

Así, varios autores coinciden en que: “...la automatización...podrá ir relevando de ello (el impulso procesal) al propio juez; dejando en mano de los sistemas informáticos estas situaciones”⁷⁹.

Esto nos llevaría a la desaparición de la cadena apelativa, dado que si la mantuviésemos, implicaría la revisión de la sentencia de una IA por otra IA de iguales características. Esto sería redundante, ya que, al aplicarse de la manera más óptima el derecho vigente, por dos IA con las misma “inteligencia” sería innecesario revisar esa sentencia.

CONCLUSIÓN

A partir de la búsqueda del satisfactorio cumplimiento de los principios de objetividad y celeridad, estas tres etapas, son las que posiblemente se darían a lo largos de los años en el proceso judicial argentino. La doctrina y el elemento normativo (el decreto antes citado), fundamentan y dan inicio al comienzo del proceso de transformación que estimamos procederá.

⁷⁹GIL, *op. cit.*, (documento digital, AR/DOC/3637/2018, p.10).

Podemos destacar que tal evolución garantizaría un mayor respeto a las garantías constitucionales (celeridad procesal, objetividad, economía procesal y tutela judicial efectiva), dando lugar a un aumento en la confianza en la justicia, en los jueces y en el sistema judicial. Además daría lugar a un manejo más eficiente y organizado, de la información disponible, que continúa en proceso de expansión.

1. BIBLIOGRAFÍA CITADA.

-CORVALÁN, Juan G., “Hacia una Administración Pública 4.0: digital y basada en inteligencia artificial. Decreto de (Tramitación digital completa)”, *LA LEY* 17/08/2018, 17/08/2018, 1; *LA LEY* 2018-D, 917, (AR/DOC/1683/2018).

-GIL, Gabriela F., “La inteligencia predictiva como herramienta de eficacia en la gestión judicial”, *SJA* 21/11/2018, 21/11/2018, 35, (AR/DOC/3637/2018).

DERECHO PENAL Y LAS NUEVAS TECNOLOGÍAS: el uso de la inteligencia artificial⁸⁰

Matías Nicolás Bares Menna⁸¹

RESUMEN

Las nuevas tecnologías suponen una forma más sencilla de ejercer nuestros derechos de libertad de expresión o de libertad de información, entre otros. Pero, a su vez, también facilitan la labor de los delincuentes para llevar a cabo las conductas que ponen en peligro otros derechos, tales como la propia imagen, la intimidad, el honor y la protección de los datos personales. Dada la concienciación de este tipo de peligros, se demandan mecanismos que ofrezcan tutela a los derechos fundamentales.

El uso de programas de inteligencia artificial como herramienta de trabajo para los jueces a la hora de determinar la predicción delictiva, es decir, la probabilidad, la peligrosidad criminal es una materia compleja porque normalmente se asocia con la aplicación de medidas de seguridad como una consecuencia jurídico penal junto con las penas y otras menos relevantes, ya no en el proceso penal, sino en el período de ejecución de la pena.

Palabras claves: Sociedad de Información; nuevas tecnologías; inteligencia artificial; delitos comunes; delitos informáticos.

80 Enlace al video <https://youtu.be/6NXz1Wic3F8>

81 Abogado UNS. Agente Judicial del Poder Judicial de la Provincia de Buenos Aires, Ministerio Público de la Defensa. Mail: matibares@hotmail.com

LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TICs)

La dimensión del problema en el derecho, es que este debe estar dotado de flexibilidad (dentro de sus posibilidades) ya que en los tiempos que corren surgen cada vez más y más formas de vulnerarlo. Esto presenta un desafío a la comunidad toda y en especial a los profesionales del derecho que ven limitados recursos propios frente a hechos flexibles y códigos rígidos, como el actual código penal.

Este nuevo paradigma dominado por las innovaciones tecnológicas apoyadas en la informática y en las redes de comunicación mundial, así como su expansión en las últimas décadas, han derivado en uno nuevo sociológico nominado Sociedad de la Información y/o del Conocimiento.

En este sentido, el conocido Informe Bangemann⁸² habla de una «nueva revolución industrial, basada en la información, que se puede procesar, almacenar, recuperar y comunicar de

82 Disponible en <http://www.rewi.hu-berlin.de/datenschutz/report.html>, en consulta realizada el 23 de agosto del 2020 en Rojo Villada, Pedro Antonio (2003): *Europa y la Sociedad de la Información: análisis del impacto del "Informe Bangemann" sobre la política, la economía y la sociedad europea en la década de los noventa*. Revista Latina de Comunicación Social, 54. Disponible en <http://www.revistalatinacs.org/200353rojo.html>

forma ilimitada e independiente de tiempo y distancia».⁸³

La información a la que tenemos la puerta abierta es tan beneficiosa, como peligrosa, por ello es necesario que el derecho penal tome medidas en el asunto, y se procure la preparación de ciudadanos y también los profesionales del sector en cuanto a esta materia se refiere, desde abogados y jueces, hasta

83 Borallo, Enrique A., en "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la Información", David Lyon "From postindustrialism to Information Society: A New Social Transformation?", *Sociology*, 20 (1986), disponible en <https://core.ac.uk/download/pdf/60634482.pdf>. Se pretende pues la superación de la "era industrial" y el intento de definición del llamado postindustrialismo. Sobre esta transformación, cf. David Lyon, "From postindustrialism to Information Society: A New Social Transformation?", *Sociology*, 20 (1986), p. 577-588; el mismo, *The Information Society: Issues and Illusions*, 1988, Cambridge: Basil Blackwell; el mismo, "The Information Society Concept in Public Policy", en Frank Gregory/Raymond Plant (eds), *Information Technology: The Public Issues*, 1989, Manchester: Manchester University Press; el mismo "Cyberspace Sociality: Controversies over Computer-mediated Communication", en Brian Loader (ed.), *The Governance of Cyberspace*, 1997, Londres-Nueva York: Routledge. Pero, como pone de relieve el propio Lyon, Postmodernidad (trad. Belén Urrutia, de la segunda edición inglesa, *Postmodernity*, publicada en 1999), 2000, Madrid: Alianza, p. 17, «en cuanto intentamos hablar de la postmodernidad tropezamos con la modernidad», esto es, de alguna manera -igual que los teóricos de la Sociedad del Riesgo (en especial Ulrich Beck), la conciben como una segunda modernidad-, algunos de los trazos de la Sociedad de la Información estarían ya dibujados en la modernidad. En el terreno jurídico, esto probablemente se corresponde con una lectura de las nuevas regulaciones como producto del evolucionismo jurídico. Sobre ello, cf., por todos, el trabajo de Porrás Nadales, en este volumen.

periodistas con un límite en los derechos humanos fundamentales.

Internet ha posibilitado que los ciudadanos de a pie tengan un acceso “prácticamente inmediato” a la información, incluyendo en este concepto tan general, a la información jurídica. Pero también ha posibilitado a los delincuentes una nueva forma de llevar a cabo actuaciones que atentan contra los derechos de los ciudadanos, poniendo en peligro numerosos bienes jurídicos.

Hacia 2011, se calculaba que más de un millón de personas de todo el mundo son víctimas diarias de la ciberdelincuencia; cada 14 segundos un adulto es víctima de un ciberdelito; y el montante anual de las pérdidas sufridas por actos de ciberdelincuencia ascienden a más de 388.000 millones de dólares (USD), lo que hace que el cibercrimen sea más rentable que el comercio global conjunto de marihuana, cocaína y heroína.⁸⁴ Esto conlleva a la toma de medidas que escapan al conocimiento del derecho en pos de la seguridad y por tal motivo tantas veces rechazadas por sus detractores. Deviene necesario el cambio entonces en

84 Datos extraídos del estudio The Symantec Internet Security Threat Report 2011 (the Norton Cybercrime Report).
http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

la forma de pensar en tratar de ajustar el derecho a los hechos y no a la inversa.

Del análisis objetivo de estos datos se observa que la tecnología ocupa mundialmente y en materia local un lugar preponderante. El Estado ha quedado prácticamente al servicio de la tecnología con normas que son de ineficaz aplicación de códigos pensados para otra época.

LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO PENAL ACTUAL

Reviste singular análisis la utilización de inteligencia artificial como modelo en el derecho penal. Particularmente debe entenderse que si bien puede resultar de gran utilidad como herramienta a la hora de analizar la probabilidad delictiva, resta consultar si la aplicación y utilización de esta en el derecho actual no enfrentaría a la estructura normativa vigente afectando derechos personales fundamentales.

Dicha programación de esta herramienta es realizada por empresas que tienen como fin codificar en una máquina “madre” perfiles que luego serán utilizados en los tribunales para así evaluar conductas potencialmente punibles.

Esto de la mano de los déficits legales actuales y como se advierten los desafíos jurídicos que representa el empleo de las nuevas tecnologías en las legítimas labores de investigación penal, a la vez que se alumbra con sólidos argumentos para instar una urgente y necesaria actualización completa de la legislación procesal adecuarse a las necesidades de la era digital y permitir el uso de las técnicas modernas de investigación que la informática ofrece, de conformidad con los Derechos Fundamentales y de los Derechos Humanos.

Veamos una cuestión de interés, en este sentido, la constituye el fenómeno de la Inteligencia Artificial en ciertos medios de comunicación, por ejemplo, donde las noticias son elaboradas íntegramente por robots, como es el caso de Heliograf , o también como ejemplo un androide de The Washington Post que redacta noticias sobre política y eventos deportivos. Pues cabe preguntarnos cuál será el marco legal en relación con los delitos de injurias y calumnias que pudiera perpetrar el dispositivo inteligente en el ámbito de su autonomía. Sin duda se trata de un tema controvertido a la par que cautivador para cualquier jurista analizar sobre quién recae su responsabilidad.

Por otro lado, al observar la experiencia europea como ejemplo de la actuación de la Inteligencia Artificial en las fuerzas de seguridad de los Estados Europeos se podría analizar sobre la afectación a los derechos fundamentales que suponían ciertas prácticas. Partimos de la idea de que esta tecnología utilizada se nutre de información masiva sobre tipos de delitos, horas del día y zonas en que se cometen para generar los llamados *hotspots* o “mapas criminales” orientados a la prevención así como a la intervención efectiva y eficiente de los profesionales de la seguridad.⁸⁵ No obstante, existen

85 Borallo, Enrique A., en “Incidencia de las nuevas tecnologías en el sistema penal”, disponible en <https://core.ac.uk/download/pdf/60634482.pdf>, cfr., (...) “De este dato interesa tanto su dimensión individual, en el sentido de que el “ciudadano electrónico” puede aspirar a múltiples contactos sin ser identificado más que por su perfil informático o internauta, como la relativa al control social, en tanto que replantea las posibilidades y medios a través de los cuales la sociedad y las agencias correspondientes aspiran a ejercerlo. Junto a ello, cabe indicar que también en otros rasgos comunes del patrón de conducta tecnológica -a saber, su virtualidad y su ambigüedad o ambivalencia o la crisis de la teoría de la acción humana, considerada como comportamiento racionalmente conducible- se advierten aspectos que pueden alcanzar especial interés jurídico-penal. En efecto, en la medida en que lo distancian del arquetipo de conducta penalmente relevante, esto es, la conducta comisiva intencional y directamente dañina del bien jurídico protegido individual, parece que se facilita la expansión de modelos de imputación “extraordinaria”, que se basan fundamentalmente en la no evitabilidad y están más cerca de las directrices que rigen las reglas de la autoría mediata, la omisión, la actio libera in causa o de la estructura de los delitos de peligro contra bienes jurídicos colectivos, etcétera(...)Se produce asimismo una estrecha convergencia de las tecnologías informáticas con las telecomunicaciones, que se impulsan mutuamente

posicionamientos críticos respecto de algunos de estos dispositivos que, además de la información a la que me he referido, se nutren de datos personales de individuos ya fichados, con la finalidad de evitar que cometan delitos (por ejemplo, el X-Law en Italia). Ello suscita recelos por parte de los defensores de los Derechos Humanos quienes se postulan reacios al manejo de esta información que, sin duda, estigmatiza a determinados individuos con antecedentes penales. Esto a la luz de los estándares de derechos humanos, como se establecen en los principales tratados internacionales y las legislaciones nacionales, imponen obligaciones a los Estados con límites en el acceso a la información privada de las personas y su disposición. Además de esta postura crítica, es importante el cuestionamiento sobre qué tipos de delitos son los que se mapean y quién decide seleccionar aquellos y no otros: ¿Puede suponer esto un modo de estigmatizar o criminalizar según qué barrios o clases sociales? Además ¿no pueden consistir estas herramientas en dispositivos de los que se valga la delincuencia para localizar la presencia policial?

generando sistemas telemáticos integrados e híbridos. Todo ello en un contexto de renovación muy acelerado”

Por otro lado, hablé sobre los usos de la Inteligencia Artificial en los órganos jurisdiccionales haciendo referencia a los algoritmos y su gestión - desarrollo. ¿Cuál es el problema? Se demostró que favorecerían según el tipo de sujetos y perjudicaban a otros con características diferentes (ejemplo son los algoritmos COMPASS O HART, en el que se detectó preferencias de personas blancas frente a personas negras, o personas ricas frente a personas pobres o de barrios pobres, respectivamente)⁸⁶. Por este motivo se alude a la necesidad de que los algoritmos sean desde su diseño y programación, hasta su utilización, transparentes en la investigación, detección y prevención del delito.

Finalmente, quiero destacar que la Inteligencia Artificial está incidiendo notoriamente sobre el ejercicio de la abogacía. Se trata de una realidad que el modelo de prestación de servicios de los abogados ha cambiado: ahora el cliente constituye el eje vertebrador de todo el proceso y las nuevas tecnologías se erigen como un aliado indispensable y fundamental para la fidelización de los clientes y la diferenciación en el mercado:

86 Disponible en:

https://retina.elpais.com/retina/2020/03/03/innovacion/1583236735_793682.html.

el exponencial crecimiento de la industria *legaltech* así lo evidencia.

Junto con ello, proliferan en el mercado herramientas de análisis predictivo que facilitan la toma de decisiones y el desarrollo de determinadas estrategias en los procesos y que pronostican las eventuales decisiones de los tribunales. He de concluir al respecto de la profecía sobre la automatización de la profesión del abogado o abogada y su posterior desaparición.

Así las cosas sólo quedará consultarnos sobre la responsabilidad ya no en manos del operador, sino de la robótica.

Veamos que el cambio de paradigma ha desarrollado la *EJUSTICE*⁸⁷ el uso de la tecnología pero no acompañado de límites claros como también sin reglas. Esto conlleva a que se excedan lo propuesto por las posturas liberales de la época que vio nacer nuestro sistema normativo.

En conclusión no será la Inteligencia Artificial la que quite el trabajo a los abogados, sino que se lo quitarán aquellos abogados que se lleven mejor con la tecnología y con la Inteligencia Artificial. Claramente abogamos por un cambio de paradigma, ajustado a reglas claras en beneficio de todas las partes,

⁸⁷ Actualidad Jurídica Iberoamericana N° 10 bis, junio 2019, ISSN: 2386-4567, pp. 792-843.

incorporando normativa al efecto que sea útil a la regulación de este nuevo mundo, en vista de nuestros pares aprendiendo de nuestros errores y aciertos.

BIBLIOGRAFÍA:

Actualidad Jurídica Iberoamericana N° 10 bis, junio 2019, ISSN: 2386-4567, pp. 792-843.

Blackwell, Basil, "The Information Society Concept in Public Policy", en Frank Gregory/Raymond Information Technology: The Public Issues, disponible en <https://venomorium.files.wordpress.com/2019/09/webster-2006-digital-society-chapter-2.pdf>.

Borllo, Enrique Anarte, en "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la Información", David Lyon "From postindustrialism to Information Society: A New Social Transformation?", *Sociology*, 20 (1986), disponible en <https://core.ac.uk/download/pdf/60634482.pdf>.

Loader Brian, "Cyberspace Sociality: Controversies over Computer-mediated Communication", *The Governance of Cyberspace*, (1997), publicado en: *Postmodernidad*, 2000, Madrid, Ed. Alianza.

EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL: UNA MIRADA A LA LUZ DEL DEBER DE MOTIVACIÓN Y DE LA AVERIGUACIÓN DE LA VERDAD SOBRE LOS HECHOS DEL CASO⁸⁸

Pablo Antonio Molina⁸⁹

RESUMEN

En el presente artículo se analizarán algunas implicancias de utilizar la inteligencia artificial en el proceso penal para la determinación de los hechos del caso.

La particularidad que presenta la utilización de este tipo de técnica de inteligencia artificial, a través de algoritmos matemáticos, radica en un alto nivel de predicción de la mano con una ausencia de explicación sobre el resultado obtenido.

En este sentido, se pretende clarificar si este tipo de prueba permite que se cumpla con el deber de motivación, en tanto dicho deber exige dar razones suficientes, formuladas lingüísticamente, que funden la decisión adoptada; y si resulta útil para alcanzar la búsqueda de la verdad sobre los hechos del caso.

Palabras Claves: Inteligencia artificial. Proceso penal. Prueba. Verdad. Motivación.

88 Enlace al video https://youtu.be/r_Ob7BeR_Hs

89 Estudiante de Derecho de la Universidad Nacional del Sur. Ayudante de Docencia B (Filosofía de la Pena y Prueba en los Procesos Judiciales) en la Lic. en Seguridad Pública UNS. Auxiliar Defensoría Penal de Bahía Blanca en el área de Ejecución Penal y Contravencional. Correo de contacto: pablomolina007@outlook.com

INTRODUCCIÓN

La inteligencia artificial ha tenido un avance notorio en el ámbito del derecho, especialmente a través de algoritmos matemáticos utilizados en aras de predecir o determinar hechos. La particularidad que presenta el uso de esta herramienta, está dada por el alto nivel de predicción, de la mano con una ausencia de explicación sobre el resultado al que se llega. Ante tal escenario, cabe preguntarse si ello contribuye a la búsqueda de la verdad y si es posible que se cumpla con el deber de motivación.

INTELIGENCIA ARTIFICIAL Y ALGORITMOS

En los últimos años la inteligencia artificial ha comenzado a utilizarse en varios ámbitos, delegándose decisiones tomadas por seres humanos en sistemas de algoritmos en áreas como la educación, la medicina, la industria, y los procedimientos de justicia (Raffo, 2019). Particularmente en este último ámbito, cobra importancia la utilización de algoritmos matemáticos en un proceso.

Los algoritmos son “(...) series de ecuaciones matemáticas que se entrelazan para proporcionar un resultado, una instrucción concreta, que sirva para solucionar un problema planteado, gracias a la consideración de un número de variables que varía sustancialmente de un caso a otro” (Iñigo & Pérez Estrada, 2019). A través de dicha herramienta se puede predecir el comportamiento de una persona o determinar la credibilidad de un testigo. Por ejemplo, el Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), un programa matemático que fue utilizado en el caso *State v. Loomis* resuelto por el Tribunal Supremo del Estado de Wisconsin de Estados se usó para determinar el riesgo de reincidencia de una persona (Garay, 2018).

Ahora bien, no hay que perder de vista que en ambos casos de lo que se trata es de probar un *hecho*⁹⁰. Es decir, en tales

⁹⁰ Rigurosamente hablando, lo que se prueba en un proceso no son en sí *hechos* sino *afirmaciones de hecho*. De tal modo, se prueba la afirmación consistente en “el testigo A miente” o “existe gran probabilidad de que la persona B reincida en el delito”. Estas *afirmaciones* sobre hechos o proposiciones fácticas, y no los *hechos* en sí, sería lo que estrictamente se prueba.

casos el algoritmo serviría como *prueba* sobre los *hechos del caso*.

Así, en la predicción de un comportamiento, se tratará de probar un hecho futuro, es decir un hecho que todavía no ha ocurrido, pero es previsible que ocurra; y en el caso de la credibilidad de un testigo, sobre un hecho presente. Podría ser posible también utilizar algoritmos para determinar un hecho pasado, si se utilizara tal herramienta para probar, por ejemplo, algún hecho relativo a la comisión de un delito.

Pero resulta importante tener en claro una particularidad esencial de tal herramienta de inteligencia artificial, la cual reside en su capacidad para predecir comportamientos, adivinar tendencias, atestiguar la verosimilitud de un testimonio, aunque teniendo como contrapartida de dicha predicción una ausencia de explicación sobre la conclusión (Iñigo & Pérez Estrada, 2019). Es decir, el algoritmo, en general, no ofrece una explicación sobre el resultado obtenido.

De este modo, la utilización de un algoritmo en el marco de un proceso podrá utilizarse para probar si un testigo miente o si es probable que una persona reincida, pero no existirá una explicación

sobre cómo se llega a dicha determinación⁹¹.

Hay excepciones, en algunos algoritmos que son sumamente sofisticados y costosos, utilizados por ejemplo en medicina, que permiten apreciar las pruebas, conclusiones y las deducciones que se han seguido para llegar a las mismas. En tal sentido, la autora Gil Elena pone el ejemplo del programa Watson Paths, que permite que los médicos vean las pruebas y el sendero de deducciones que ha seguido el ordenador para lanzar sus conclusiones (por ejemplo, cómo ha concluido el diagnóstico médico que realiza) (Gil, 2015). Pero fuera de este caso, la gran mayoría no presenta tales cualidades.

Frente a tal panorama es preciso indagar qué sucede con la búsqueda de la verdad, fin ideal de todo proceso, y el deber de motivación, cuando se utiliza un algoritmo que no permite seguir el camino lógico que conllevó a la determinación de un hecho.

⁹¹ La única explicación que podría darse sería aquella consistente en que un determinado hecho se tuvo por probado porque se utilizó un algoritmo inteligente que otorgó gran probabilidad de que dicho hecho haya ocurrido o vaya a ocurrir. Sin embargo, lo que seguirá sin explicación es cómo fue que se llegó a la conclusión determinada por dicho algoritmo.

VERDAD DE LOS HECHOS Y MOTIVACIÓN

Como lo sostiene Ferrer Beltrán “la búsqueda de la verdad es un elemento imprescindible para un proceso garantista de derechos”, resultando así un objetivo estructural de la actividad probatoria en todo proceso (Ferrer Beltrán, 2020).

En este sentido, la utilización de algoritmos inteligentes como prueba en el marco de un proceso, por el alto nivel de predicción que poseen, podría colaborar eficazmente a alcanzar la verdad sobre los hechos. Contribuyendo así, eficazmente a garantizar uno de los objetivos primordiales en todo proceso.

Sin embargo, la averiguación de la verdad no es el único objetivo ni debe obtenerse a cualquier costo. También existen otros bienes considerados valiosos dignos de tutela. Verbigracia, la búsqueda de la verdad debe ceder si el procedimiento para obtenerla implica torturar a la persona que se indaga. Es por ello que cuando se habla de buscar la verdad, de lo que se trata es de un ideal a alcanzar.

Precisamente, uno de los bienes dignos de tutela radica en el derecho de que la decisión judicial esté motivada. En cualquier tipo de proceso, pero en especial en el penal, cobra suma

importancia la exigencia de motivación en la decisión del juez que determina como probado un hecho. Tal deber es una garantía frente a la arbitrariedad, que deriva del art. 8.1 de la Convención Americana de Derechos Humanos⁹².

En relación a este punto, Ferrer Beltrán (Ferrer Beltrán, 2020) diferencia entre distintos tipos de motivación. Por una parte, el referido autor menciona que la motivación psicologista tiene que ver con la expresión lingüística de los motivos (causas) que han llevado a una decisión, como el contexto social, el estado de ánimo del juez, etc. Frente a ella, la motivación de tipo racionalista implica una justificación de la decisión judicial, es decir se trata de aportar razones que la justifican. En este último tipo de motivación, se distingue según que haya razones suficientes que funden la decisión o que, además de existir dichas razones,

92 De tal modo, la Corte Interamericana de Derechos Humanos ha sostenido que “el deber de motivación es una de las ‘debidas garantías’ incluidas en el artículo 8.1 para salvaguardar el derecho a un debido proceso” (Corte IDH., *Caso Apitz Barbera y otros (“Corte Primera de lo Contencioso Administrativo”) Vs. Venezuela*, párr. 78). Asimismo, ha precisado que la motivación “es la exteriorización de la justificación razonada que permite llegar a una conclusión” (Corte IDH., *Caso Chaparro Álvarez y Lapo Íñiguez Vs. Ecuador*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 21 de noviembre de 2007. Serie C No. 170, párr. 107) y conlleva una exposición racional de las razones que llevan al juzgador a adoptar una decisión.

las mismas hayan sido formuladas lingüísticamente de modo analítico (expresadas en la sentencia).

El tipo de motivación que permite garantizar el debido proceso ante jueces profesionales, exige formular lingüísticamente las razones que fundan una decisión. La relevancia de esta garantía se encuentra ligada a la correcta administración de justicia y a evitar que se emitan decisiones arbitrarias, otorgando, además, credibilidad de las decisiones jurídicas en el marco de una sociedad democrática y demostrando a las partes que éstas han sido oídas⁹³.

En vista de lo anterior surge el interrogante de si es posible que se cumpla con dicha exigencia, en el hipotético caso de contar con un algoritmo inteligente como prueba esencial en el marco de un proceso penal.

Como se dijo anteriormente, a través de tal prueba podría determinarse como probado un hecho, pero no podría ofrecerse ninguna explicación sobre cómo se llegó a dicha conclusión, con lo cual, es evidente que el deber de motivación, en los términos que han sido explicados, se verá seriamente menguado.

Ello así, toda vez las razones que se expresarán como suficientes y que fundarán la decisión, se limitarán a la existencia de un algoritmo que determinó como probable la ocurrencia de un hecho, pero sin poder explicar cómo se ha llegado a dicha determinación. Tal como lo sostiene Ferrer Beltrán, demasiadas veces se confunde motivación con descripción de pruebas admitidas, pero ello no cumple con las exigencias de una concepción racional de motivación (Ferrer Beltrán, 2020).

La concepción racional de motivación, exige la exteriorización de la justificación razonada que permite llegar a una conclusión y conlleva una exposición racional de las razones que llevan al juzgador a adoptar una decisión. Esto se vincula, a la necesidad de las partes de conocer las razones de la decisión de culpabilidad o inocencia, permitiéndoles comprender el resultado del proceso como una consecuencia racional de la prueba incorporada. Tal justificación razonada, se verá menguada en el caso de contar con un algoritmo que determina como muy probable la ocurrencia de un hecho, pero sin ofrecer una explicación sobre cómo fue que se llegó a esa determinación.

93 Corte IDH., *Caso V.R.P., V.P.C. y otros vs. Nicaragua*, sentencia de 8/3/2018, párr. 254

En tal situación se vería afectado también el derecho al recurso, ya que la parte que pretenda recurrir la decisión judicial se vería imposibilitada de conocer las premisas fácticas que llevaron a la determinación del hecho por parte del algoritmo. Es decir, no se sabría por qué el algoritmo determinó, por ejemplo, un hecho consistente en “la persona ‘b’ reincidirá”. Así, es evidente que la posibilidad de interponer un recurso se ve seriamente restringida.

Ante ello, la utilización de algoritmos como prueba en el marco de un proceso, en tanto no resulte posible conocer las razones que llevaron a la determinación de un hecho, trastoca el deber de motivación y afecta la posibilidad de recurrir de las partes.

Para hacer frente a la arbitrariedad resulta sumamente importante utilizar mecanismos que permitan conocer el camino lógico que ha llevado a un determinado resultado, a fin de controlar adecuadamente la decisión adoptada. Tal como, por ejemplo, el mencionado programa Watson Patsh al que alude la citada autora Gil Elena, que permite que los médicos vean las pruebas y el sendero de deducciones que ha seguido el ordenador para lanzar sus conclusiones (Gil, 2015).

CONCLUSIONES

Con lo cual, la utilización de algoritmos inteligentes en el marco de un proceso penal podría considerarse una herramienta útil a los fines de alcanzar la verdad sobre los hechos.

Sin embargo, en tanto no se pueda ofrecer una explicación sobre cómo fue que se llegó a la determinación sobre un hecho, dicha circunstancia restringirá la posibilidad de motivar adecuadamente la decisión judicial y de recurrir la decisión. Toda vez que la formulación de razones que funden la misma se limitarán a la existencia de tal prueba como determinante de un hecho, quedando sin explicar por qué se llegó a tal determinación.

Es por ello que, para impedir tal arbitrariedad, resulta sumamente importante utilizar mecanismos que permitan conocer el camino lógico que ha llevado a un determinado resultado, a fin de controlar adecuadamente la decisión adoptada.

BIBLIOGRAFÍA

- Ferrer Beltrán, Jordi, “Sobre el deber de motivación de las decisiones probatorias y el juicio por jurados. La sentencia V.R.P.,

V.P.C. y otros vs. Nicaragua de la CortelDH”, *Questio facti. Revista Internacional sobre Razonamiento Probatorio*, N. 1, Ed. Marcial Pons Ediciones Jurídicas y Sociales, ISSN: 2604-6202, Madrid, 2020, pp. 359-382.

- Garay, Lucía Martínez, “Peligrosidad, algoritmos y *due process*: el caso *State v Loomis*”, *Revista de derecho penal y criminología*, 3ª Época, n° 20, Julio de 2018, p. 490.

- Gil, Elena, “Big data, privacidad y protección de datos”, XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, 2015, Agencia

Estatal Boletín Oficial del Estado, Madrid, 2016, pp. 28 y 43.

- Iñigo de Miguel Beriain y Miren Josune Pérez Estrada, “La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados”, *Revista de Derecho UNED*, núm. 25, 2019, p. 335.

- Raffo, Francisca Emilia, (2019). “Nuevas tecnologías y derecho penal: la responsabilidad penal en la era de la inteligencia artificial”. Universidad de San Andrés, Buenos Aires, 31 de julio de 2019.

LA APLICABILIDAD DE MACHINE LEARNING EN LOS JUZGADOS DE ARGENTINA ¿UNA POTENCIAL HERRAMIENTA EN EL ACCESO A LA JUSTICIA?⁹⁴

Elian Facundo Yorlano⁹⁵

RESUMEN

En nuestra actualidad mundial nos estamos encaminando hacia una inserción cuasi total de la tecnología en nuestro cotidiano. Y el ámbito jurídico no escapa a ello. Dentro de estas cuestiones, encontramos una rama de la inteligencia artificial, controvertida al ingresar en el mundo profesional: Machine Learning.

Es utópico en lo inmediato pensar un sistema que prediga resoluciones o sentencias, por medio de la carga de algoritmos a través de análisis de datos. Sin embargo, la legislación comparada demuestra distintos modos de aplicación paulatina.

En Argentina surge el interrogante para saber si nos encontramos ante una herramienta que aún no se ha desarrollado lo suficiente en nuestro país o si el machine learning configuraría una quimera la cual nunca llegará a incorporarse a nuestros juzgados. ¿Estamos omitiendo una herramienta que puede ser esencial en el futuro acceso a la justicia? ¿Encontraríamos la deseada celeridad judicial si la función magistrada es acompañada con el uso de machine learning?

Palabras claves: Inteligencia Artificial - Machine Learning - Acceso a la Justicia - Tareas jurídicas

94 Enlace al video <https://youtu.be/av6xGLZJ0Kk>

95 Abogado egresado de la Universidad Nacional de La Plata - Contacto: efacundoyorlano@gmail.com

INTRODUCCIÓN:

Día a día somos sorprendidos por las novedades que se manifiestan en el mundo sobre la conjunción del territorio jurídico y la tecnología. “*Ross, el abogado robot, lleva más de un año trabajando en la firma Baker & Hostetler en Estados Unidos*” nos afirman desde el norte del continente americano. En el año 2018, numerosos medios comunicaban anonadados “*Donotpay, una app para demandar a alguien desde el móvil*”. (As.com, 2018)

Para algunos, estamos viviendo en tiempos dignos de ser catalogados como una novela distópica de George Orwell, encaminándonos hacia un futuro donde el ser humano será prescindible y las máquinas, con sus algoritmos y mecanización, (exentas de la exigencia de un salario, del cansancio del cuerpo y otros “desperfectos” en pos de la productividad) realizarán el trabajo que hoy realizamos. ¿Una potencial extinción del hombre? Algunos creen que, en varios años, gran parte de las consultas legales se realizará en línea. (Oppenheimer, 2018)

En cambio, para otros, nos encontramos en la era de las posibilidades. Allí donde la tecnología esta al servicio de la humanidad para potenciar nuestras habilidades, no para opacarlas ni mucho menos sustituirlas. Utilizar medios innovadores para facilitar el trabajo de la persona quizás permita dejar de preocuparnos en hacer trabajos automáticos.

Y aquí se encuentra la base de este cuestionamiento: ¿Cómo aplicar la rama de la Inteligencia Artificial (IA a partir de aquí) conocida como Machine Learning a la profesión jurídica (en su sentido más amplio)?

Para comenzar, podemos afirmar de manera concisa que *Machine Learning* es una rama de la IA aplicada que trata de lograr que las máquinas incorporen de forma automática, a través de un aprendizaje de entrenamiento de algoritmos, para que, a partir de patrones obtenidos del análisis de datos, realicen predicciones perfeccionando modelos que nos ayuden a generar ideas y tomar mejores decisiones. Cuantos más datos haya disponibles para aprender y más rico

y completo sea el algoritmo, funcionará mejor. (Molina Pérez - Tomé, 2018)

Ahora bien, ¿cómo aplicar este aprendizaje automático en el Derecho? ¿Cómo se vería aplicado en los juzgados de Argentina? ¿Significarán un catalizador en la tan ansiada búsqueda del acceso a la justicia? ¿Proveerán herramientas certeras para aplicar el Derecho de una manera más justa (no sólo en cuanto a resultado, sino también en referencia a la celeridad)? Ya que “la justicia que es lenta no es justicia”. ¿Es sostenible un modelo que no incorpore la tecnología paulatinamente en los tiempos que corren? El número de interrogantes que surgen es directamente proporcional a la cantidad de oportunidades que se presentan.

Antes de comenzar a hablar de la posible inserción del machine learning, es dable tener en cuenta dos premisas fundamentales: La actividad jurídica es una actividad humana, y que en gran parte depende de la capacidad de razonar y de sentir de las partes involucradas. En segundo lugar, la innovación en cuestiones tecnológicas, de IA y de experiencias automáticas como el machine learning, sólo podrán ser útiles al hombre en tanto y en cuanto tengan vocación colaborativa y no sustitutiva.

Habiendo establecido los parámetros necesarios para avizorar cómo el machine learning puede ser compatible con nuestro sistema de justicia, será de gran ayuda ver algunos ejemplos de la práctica.

- **PROMETEA**, un sistema argentino de IA multicapa, desarrollado en conjunto por el MPF de la CABA y la Facultad de Derecho de la UBA. Su función es evitar a los funcionarios judiciales la realización de tareas repetitivas, permitiéndoles focalizar su trabajo en los casos complejos, en los que se hace más necesario el trabajo humano, tanto para el análisis y escritura de fallos, como para aspectos como la contención de víctimas, que sólo podrían ser llevadas a cabo por un humano. (lalab, 2019)

- **PRETORIA**, sistema de IA basado en Prometea. Desde Colombia explican que puede leer, detectar, predecir y elaborar resúmenes sobre miles de sentencias en pocos segundos. “Para tener en cuenta la agilización, se calcula que una persona demora, en promedio, en leer y armar un resumen sobre una sola sentencia unos 27 minutos”, explican los creadores de este sistema. Y la Corte recibe, en promedio, 2700 amparos por día. (Oquendo, 2020)

- **COMPAS**, un sistema de herramienta de casos y decisiones desarrollado en U.S.A. y utilizado en sus Cortes para calcular la posible reincidencia de un imputado, a través de diferentes escalas: *Pretrial Release Risk*; *General Recidivism* y *Violent Recidivism*. (Washington, Anne L. 2019)

El *machine learning* no discrimina en cuanto a utilidad para fueros. Como en los ejemplos descriptos, alrededor del mundo se está inmiscuyendo en lo penal, civil, laboral, previsional, y con utilidades a veces impensadas en un tiempo, que mutan según las necesidades e innovaciones.

En cualquiera de las diversas posibilidades jurídicas que puede asumir, se debe constituir un sistema. En mi opinión, este debe contener, en el caso argentino (aplicable en otros ordenamientos nacionales) **3 principios** que deben estructurar estos novedosos mecanismos (Economía, coyuntura y propósito humano), concretados a través de **3 redes** que les corresponden (Discriminación de tareas, Inversión humano – económica y Capacitación) que formarán un entramado desembocando

en **una sola consecuencia lógica** (Acceso a la justicia).

Para comenzar, es una premisa obvia que la innovación de sistemas y la incorporación de tecnología traerán consigo una celeridad en el sistema judicial. Por ejemplo, una computadora de última generación conlleva un ahorro de tiempo para quien la utilice. Pero en el sistema de inserción de *Machine Learning* en nuestra justicia, el principio de **economía** va un poco más allá. Significa economizar al máximo los tiempos de los jueces y funcionarios judiciales, evitando que realicen tareas monótonas que podría efectuar un dispositivo al modo *check in* (por ejemplo, es bien sabido que, aún en la era de la digitalización del sistema judicial, un auto de apertura sucesoria puede tardar varias semanas, cuando es una resolución simple si están cumplidos los requisitos que dispone el actor). Este ahorro de tiempo se traduce en más dedicación a otras causas que merecen pronto despacho, que necesitan de la capacidad de razonar y decidir del magistrado. Carnelutti postuló que las decisiones del juez provienen de su íntima convicción y luego las fundamenta con doctrina para argumentar el sentimiento. (Carnelutti, 1936) Y en muchos casos la realidad se condice. Pero no en las tareas monótonas, en las cuales se podría

aplicar el principio de subsidiariedad para que el *machine learning* se encargue.

Esto, por añadidura, se traduce en agilidad para los abogados y sus clientes, es decir, la sociedad que busca justicia.

Conexo a lo expuesto, es importante resaltar lo mencionado hace algunos párrafos. Toda cuestión novedosa que irrumpa en un sistema tradicional, como lo es el jurídico, tendrá tintes disruptivos, pero que no deben obstruir la visión de su función instrumental. No estamos hablando de sistemas que reemplacen paulatinamente la función jurídica, sino que haya una **coyuntura** tecnológica – humana. Esto es así porque mucho se ha hablado de la posible “sustitución” de las profesiones tradicionales (como la abogacía) por el exponencial crecimiento de la tecnología, el cual no deja de ser cierto, pero que podemos tomarlo en una faz integradora más que reemplazante. El acompañamiento de la máquina (en su sentido más amplio) al operador jurídico sólo podrá ser provechoso si hay una complementariedad (no recíproca, por la dignidad humana que nunca alcanzará un dispositivo) sino en la faz profesional.

El último de los principios es plenamente explícito. El machine learning aplicado en nuestra justicia debe tener esencialmente un **fin humano**. ¿De qué otra manera

podemos pensar una mejora en el sistema judicial?

Ahora bien, en este entramado que se ha creado a fin de manifestar la necesidad de incorporar mecanismos que propicien la búsqueda de justicia, donde teorizamos una inserción regida a base de los 3 principios expuestos, vemos que hay 3 redes o medios por los cuales los principios se interrelacionan constantemente, donde hay un medio por cada principio, pero donde también hallamos una constante interrelación. En concreto, en cuanto a economía nos referimos, precisamos de una **inversión económico – humana**, seguida de una **capacitación** constante, lo cual podría corresponderse con la ya mencionada coyuntura que implica una relación permanente entre el hombre y la tecnología innovativa. Y como ya hablamos del fin humano que debe necesariamente tener este proceso, también podemos hablar de la **discriminación de tareas** que no debe desdibujarse.

Con los ejemplos de Prometea, Pretoria y Compas, vemos una estimación de cómo estas novedosas herramientas pueden insertarse en nuestro día a día jurídico. Habrá una inversión inicial, donde en el caso de los Juzgados, deberá ser

soportada por el Estado que disponga el capital económico a fin de adquirir los sistemas necesarios, pero también conjugará con la inversión humana, ya que debe haber personas no sólo que hagan uso sino también que reparen y programen. Empezaremos a hablar (aunque ya está instalado el tópico) de una interdisciplinariedad profesional entre el derecho y la informática. Donde además del servicio técnico también podrán otorgar la capacitación necesaria y constante para el uso de los dispositivos *machine learning* a fin de ser utilizarlos en una forma provechosa.

Por último, la discriminación de tareas tiene que ver con todos los demás puntos. Es importante desde el inicio de la adquisición de un sistema, tener en claro qué tareas realizará, la manera, y qué beneficio traerá al sistema de justicia. Delegar tareas monótonas o “automáticas” que hoy en día son realizadas por los funcionarios judiciales podría ser la mejor opción. Sin embargo, hay que ver cuáles son estas, que variarán con el fuero, la cantidad de personal, el tráfico de causas y demás.

Todo esto, de una forma bien encaminada, teniendo no otra meta que el bien común, nos llevará a poder alcanzar, o al menos estar un poco más cerca que

en la actualidad, al tan ansiado **acceso a la justicia**.

Conociendo de manera más profunda al *machine learning* aplicado en el sistema judicial argentino, el paso siguiente es diagnosticar las problemáticas y programar al corto plazo su inserción, teniendo en cuenta la constante innovación.

En nuestra sociedad, se necesita garantizar el acceso a la justicia que profesa el artículo 16 de la Constitución Nacional. Si se da una verdadera celeridad en los procesos judiciales, todos seremos beneficiados. Que una madre desempleada con dos hijos pueda recibir la respuesta a su amparo para cobrar un subsidio en un día, es verdadera justicia. El acceso a la justicia de aquellos que antes no podían hacerlo por falta de recursos (ya sea la lentitud de los juzgados que impedía cobrar a tiempo determinados montos decisivos en la vida de la persona); la agilización de los procesos penales (teniendo en cuenta la gravedad que significa estar encarcelado cuando se es inocente); la rápida reinserción o indemnización laboral de un desempleado arbitrariamente. Esos casos son verdadera justicia, y el *machine learning* puede contribuir a alcanzar estos logros.

BIBLIOGRAFÍA

- IALAB (2019). Prometea: Inteligencia Artificial al servicio de la administración.
- Oquendo, Catalina (2020) Inteligencia artificial para desatascar la justicia en Colombia. Diario Retina
- Washington, Anne L. (2019) How to argue with an algorithm: Lessons from the COMPAS ProPublica Debate. NYU Steinhardt
- Carnelutti, Francesco (1936) El elogio de los jueces. Ed. Flores.
- Pérez Tomé, Sara Molina (2018) Machine Learning en el sector Legal. Revista del Consejo General Abogacía Española
- Oppenheimer, Andrés (2018) ¡Sálvese quien pueda! El futuro del trabajo en la era de la automatización. El futuro de los abogados, contadores y aseguradores. Editorial Debate.

DIGITALIZACIÓN DEL PODER JUDICIAL, EL DESAFÍO DE CUIDAR LA DIGNIDAD⁹⁶

Flammini Marina⁹⁷ y Liceda Ernesto⁹⁸

RESUMEN:

Con la digitalización del poder judicial, y aún más en el marco de la emergencia sanitaria conocida por todos, fueron evidentes los avances en relación al derecho a la información, control ciudadano de los actos de gobierno y acceso de justicia. Pero no debemos perder de vista las consecuencias que sobrevinieron ante la presencia de los múltiples tipos de información coexistentes en el expediente judicial digital, lo cual dejó expuesto el avasallamiento a la dignidad de los ciudadanos al dejar ante un acceso casi irrestricto a datos de carácter sensible. El presente trabajo comprobará la manera en que la digitalización del poder judicial no tuvo en cuenta la protección de estos datos, y que sólo se hizo una distinción en cuanto a fueros, desatendiendo las categorías de información en relación a los niveles de acceso necesarios para el acceso o protección respecto de a la misma.

Palabras Claves: Protección de datos personales – Seguridad de la información- Expediente Digital

96 Enlace al video <https://youtu.be/t7fXOPZNMKI>

97 Abogada. Docente de Seminarios Digitalización de Poder Judicial. Integrante del GECSI-FCJyS-UNLP mail: mflammini@gmail.com

98 Abogado. Docente Investigador GECSI-FCJyS-UNLP mail: eliceda@gmail.com

INTRODUCCIÓN Y DESARROLLO

Podemos decir que, en el poder judicial de la provincia de Buenos Aires, la publicidad por medios informáticos comenzó con la Mesa de Entradas Virtual (en adelante MEV), una plataforma multi-fuero y multi-instancia que los juzgados y tribunales fueron incorporando, en concordancia con lo estipulado por la Resolución N°31/991 de la Suprema Corte de Justicia de la Provincia de Buenos Aires (SCBA), la cual disponía que tanto los juzgados civiles y comerciales como los tribunales del trabajo, debían realizar la carga completa de datos de los expedientes judiciales en el sistema de gestión e información, a los fines de permitir visualizar el estado de cada trámite cumplido.⁹⁹

Obviamente éste fue uno de los pasos necesarios para la digitalización del expediente judicial, lo que se vio materializado a través del uso de distintas tecnologías de la información y la comunicación. Fortaleciendo de este modo el derecho a los litigantes y letrados al acceso a la información pública y a la transparencia de los actos de gobierno en

relación a las diversas causas que tramiten por ante órgano jurisdiccionales de la Provincia de Buenos Aires.

En lo que respecta al acceso de datos e información es pertinente resaltar una distinción en función al fuero al que pertenezcan los expedientes. En el fuero de familia se protege desde siempre (o al menos se intenta) la intimidad personal y del grupo familiar, por lo que su sistema de acceso es restringido debiendo solicitarse el permiso correspondiente para poder visualizar un expediente específico. Los legitimados para acceder al mismo serán las partes, sus letrados, el Ministerio pupilar y terceros debidamente autorizados. Todo ello fundamentado por la resolución n° 545/06 de la Suprema Corte de Justicia, la cual estableció un sistema de protección de datos por el cual el acceso informático a la causa es autorizado por el Juzgado, con la finalidad de controlar que la causa sea consultada sólo por los legitimados. En cuanto a las sentencias, se mantiene la privacidad y a los efectos de difundir los criterios y sentar jurisprudencia se lleva a cabo un proceso de disociación de las personas involucradas mediante la utilización de iniciales para los nombres y apellidos.

Por su parte, en el fuero penal predomina el principio de publicidad, que podrá ser

⁹⁹ La Resolución 2234/142: "(...)la implementación de las Mesas de Entradas Virtuales tiene una directa repercusión en la eficiencia del servicio de justicia, reduciendo los tiempos (arts. 15 de la Constitución Provincial; 18 de la Constitución Nacional; 8 de la Convención Americana de Derechos Humanos)

reevaluado durante la etapa de investigación en los casos en que la publicidad las actuaciones pueda ponerla en peligro. En lo que respecta al acceso mediante la MEV a la causa y a los elementos probatorios, debe solicitarse la autorización, pudiendo -en principio- acceder solamente el imputado, su defensa y los auxiliares designados en el proceso judicial.

En el resto de los fueros se hace presente un acceso – a casi la totalidad de los expedientes- a quien cuente con usuario en dicho sistema, posibilitando entonces el control ciudadano de los actos realizados por el Estado, las decisiones de éste y los tiempos de los distintos procesos. Cabe preguntarnos si esta fue la intención de la Suprema Corte de Justicia de la provincia al momento de su creación. Al respecto, Díaz Cafferata (2009) plantea en relación a esta temática que “el derecho de acceso a la información pública es una figura relativamente novedosa, y con una configuración parcialmente distinta en los diferentes sistemas jurídicos que la han receptado”, tal vez podríamos incluir en dicha definición que no sólo puede tener diversas configuraciones sino que también puede ser considerado un efecto colateral.

Previo adentrarnos más en esta temática, creemos necesario destacar las clasificaciones sobre la información planteadas por Vivant (1993), quien enumera tres tipos de vínculos entre la información y el nivel de acceso: A) La información reservada, que puede ser de interés público o privado, y cuenta con controles en sus niveles de accesibilidad. Para poder acceder a ella es necesario solicitar permiso. B) La información accesible, es aquella a la que se puede acceder, aunque no necesariamente se deba acceder. Y C) La información común o pública, donde la información tiene por fin ser difundida, pertenece al ámbito público (fundamentada en la publicidad de los actos de gobierno, control de los jueces, transparencia, entre otros).

Ya en este punto, podemos adelantar entonces que, como contracara de este avance, se hizo presente el avasallamiento de derechos personalísimos como la intimidad y la privacidad, comprendidos en el derecho a la dignidad de las personas.

Por lo aquí expuesto, nos vimos impulsados a efectuar un trabajo de campo exploratorio en el marco del proyecto de investigación que estamos

llevando adelante¹⁰⁰, con el objeto de determinar las posibilidades de tomar vista de los expedientes en los distintos fueros y comprobar cuáles son los niveles de acceso/seguridad con los que nos encontramos al momento del ingreso al sistema y en específico al tomar vista del expediente a través de la MEV.

Existen dos tipos de usuarios básicos en la MEV, uno con el rol de particular y otro de abogado donde se deben cargar, además de los datos solicitados al particular, los datos referidos a la matrícula profesional.

Comenzamos con una primera aproximación de campo, estableciendo algunas palabras claves para efectuar búsquedas dentro del sistema (las cuales se preservaran en esta etapa del proyecto, para preservar la dignidad de las personas involucradas).

Posteriormente, se llevó adelante un primer ingreso a la MEV desde un usuario “real” con el rol de abogado, utilizando las palabras clave previamente seleccionadas. Se ingresó al azar a algunos de los expedientes que el sistema arrojaba como resultado de la búsqueda

realizada con las palabras claves. Esto permitió acceder a múltiples datos personales y sensibles. Las únicas limitaciones presentadas fueron la falta de carga de la información en el sistema, y no restricciones de acceso o privacidad.

Una vez establecido el nivel de acceso que se podía lograr mediante el perfil con rol de abogado se realizó un nuevo ingreso, esta con el usuario con rol de particular, siguiendo las mismas acciones y los resultados fueron idénticos a los anteriormente detallados. Es decir, desde un usuario de rol particular y sin ningún mecanismo de autenticación sobre los datos brindados al momento de crearlo, el equipo logró acceder no sólo a los datos personales de las partes y de terceros - como domicilio, propiedades, partidas de nacimiento, etc-, sino también a datos sensibles, tales como enfermedades, consumo de medicamentos, tiempo y lugares donde algunos de los sujetos del proceso fueron internados, entre muchos otros datos relevantes y sensibles.

Debemos tener presente que conforme a la ley 25.326 de protección de datos personales, los datos sensibles deben ser objeto de un tratamiento diferente al de los datos personales, lo que evidentemente no ocurre en la MEV. Además recordar que la citada ley en su

¹⁰⁰ Proyecto I+D J183: “Servicio de justicia y gestión en contexto de las tics: antecedentes, desarrollo, expansión y proyección de la digitalización en el servicio de justicia relacionada a los Derechos Humanos de cuarta generación”. Director: Prof. Mario Silvio Gerlero UNLP

art. 5 inc. 2. a. establece que *“No será necesario el consentimiento cuando: Los datos se obtengan de fuentes de acceso público irrestricto”*, ello vinculado a la licitud del tratamiento de datos personales. Entendiendo que el acceso es irrestricto en tanto sólo requiere la creación de un usuario “simple” para el acceso a la generalidad de los expedientes esto configura una grave violación a la dignidad de los justiciables pudiendo ser objeto de su tratamiento por parte de terceros totalmente ajenos a las diversas causas, con fines distintos para los que fueron brindados por los ciudadanos.

PRIMERAS CONCLUSIONES

- 1.- El sistema MEV puede ser considerado “una fuente de acceso público irrestricto” conforme al art. 5 inc. 2. a. ley 25326, ello como premisa y adelanto de los resultados del presente proyecto, excluyendo a los fueros de familia y penal.
- 2.- Avisoramos que no se han tenido en cuenta la preexistencia de los límites físicos ni los resultantes de la interacción humana para el acceso a aquellos expedientes que contengan datos sensibles (conf. art 2 ley 25326).

La facilidad y falta de obstáculos para poder acceder a este tipo de datos o información nos lleva a pensar que, antaño, los empleados judiciales de “mesa de entradas” podían ejercer cierto control respecto de determinados expedientes, pero ello no sucedió al acceder a los mismos a través de la MEV.

3.- Advertimos que no se idearon medidas para mitigar esta falta de “filtros” o protecciones.

Consecuentemente, creemos necesario el logro de un equilibrio entre la accesibilidad, la “transparencia” y la dignidad de las personas involucradas en los diversos expedientes, en concordancia con el respeto de sus derechos individuales.

4.- Entendemos que sería deseable la creación de protocolos de seguridad de la información donde, se determinen cuidadosamente las categorías de la información (o datos), el tratamiento y los permisos de acceso. O como alternativa posible, proceder a la disociación de los datos en los expedientes evitando de esta manera el avasallamiento a la dignidad de las personas involucradas en los procesos judiciales.

BIBLIOGRAFÍA

- Díaz, Alejandra Patricia “El Control De La Actividad Estatal: Las Herramientas De La Información” (disponible en <http://www.derecho.uba.ar/docentes/pdf/el-control-de-la-actividad-estatal-ii/cae2-diaz.pdf>)

- Díaz Cafferata, Santiago, “El derecho de acceso a la información pública. Situación actual y propuestas para una ley”; en Lecciones y Ensayos, Revista de la Facultad de Derecho de la UBA, Nº 86, 2006, p.153. (Disponible en:

http://www.derecho.uba.ar/publicaciones/ye/revistas/lecciones_y_ensayos_nro_008_6.pdf)

- Vivant, Michel: “Derecho de la información. Un derecho de acceso: ¿hasta dónde?”, Derecho de Alta Tecnología, Año V, no 55, marzo de 1993, p. 1.



Capítulo 4

Las Tecnologías Digitales en los Procesos de Administración de Justicia



PANDEMIA: TIERRA FÉRTIL PARA LA INSTAURACIÓN DE LA FILOSOFÍA DIGITAL EN EL ÁMBITO JUDICIAL¹⁰¹

María Fernanda Díaz¹⁰²

RESUMEN

Tras la paralización del servicio de justicia durante los primeros estadios del ASPO, se evidenció el atraso científico-tecnológico y estructural en la escena judicial y la necesidad de superar la cultura analógica para pasar a una de neto corte digital.

El escenario actual plantea la oportunidad de modernizar el sistema para hacer frente a los desafíos que impone el siglo XXI: una justicia eficiente, innovadora y proactiva.

Se presenta la digitalización, entonces, como derecho de la ciudadanía -en términos de optimización temporal y aumento de productividad de la actividad de los órganos jurisdiccionales- para acceder a respuestas de calidad en el marco del proceso.

Frente a un nuevo paradigma, la implementación de las TICs importa un pilar primordial para entender la justicia del porvenir.

Palabras claves: ASPO, analógico, digital, productividad, proceso.

101 Enlace al video https://youtu.be/O_vlB3Slpi4

102 Abogada, UNLZ. Integrante de Ateneo de Derecho Procesal “Dr. Ruben Carlos Egozcué”. Colegio de Abogados Departamento Judicial de Trenque Lauquen.- mail: mfd_89@hotmail.com.ar

I

INTRODUCCIÓN:

Tras la paralización del servicio de justicia durante los primeros estadios del aislamiento social preventivo y obligatorio, se evidenció el atraso científico-tecnológico y estructural en la escena judicial y la necesidad de superar la cultura analógica para pasar a una de neto corte digital.

El escenario actual plantea la oportunidad de modernizar el sistema para hacer frente a los desafíos que impone el siglo XXI: una justicia eficiente, innovadora y proactiva.

Se presenta la digitalización, entonces, como derecho de la ciudadanía -en términos de optimización temporal y aumento de productividad de los órganos jurisdiccionales- para acceder a respuestas de calidad en el marco del proceso.

Frente a un nuevo paradigma, la implementación de las TICs importa un pilar primordial para entender la justicia del porvenir.

ESTADO DE COSAS: DESAFÍOS ACTUALES PARA LA HUMANIDAD

El panorama planteado en estos tiempos posee varias aristas.

Por un lado, somos testigos de una desigualdad creciente. Asimismo, el desempleo no da tregua.

En el orden colectivo, se evidencia un déficit de liderazgo que debilita las democracias y la pronunciación cada vez más frecuente de términos tales como “cambio climático” y “catástrofes naturales”, ya no producen alarma alguna (*ETHICS España, 2014*).

Mientras que la brecha de ingresos destruye el sueño “*self-made*” de la clase media, se evidencia un divorcio ostensible entre la agenda política y la realidad del ciudadano común.

En tamaño contexto, el hombre actual requiere de líderes que posean naturaleza proactiva y perspectiva global; pero por sobre todas las cosas, credibilidad, coraje y empatía.

Tradicionalmente, los gobiernos han mantenido a la ciudadanía al margen de las decisiones públicas, no siendo una excepción a ello la Justicia.

La pandemia, en tanto catalizador de una revolución socio-tecnológica, se presenta como oportunidad para mejorar el servicio

de justicia brindando apertura, cercanía, diálogo, eficacia y transparencia.

EL EXPEDIENTE ELECTRÓNICO COMO GARANTÍA DE LA TUTELA JUDICIAL EFECTIVA

Sin perjuicio del largo camino que queda por recorrer en nuestro país en términos de digitalización del ordenamiento judicial, hemos presenciado en los últimos tiempos cuantiosos cambios relativos a la tramitación del proceso.

En ocasión de celebrar una audiencia, incorporar elementos probatorios y notificar resoluciones, entre tantos otros actos procesales, la aplicación de las nuevas tecnologías importa soluciones a cuestiones trascendentales tales como la optimización de tiempo y recursos.

En pos de asegurar la tutela judicial efectiva, parecen adquirir –en este contexto- mayor relevancia una gama de principios procesales que resultan conducentes a la materialización de aquélla. A saber: celeridad, concentración, coordinación y eficacia, atravesados por una óptica permeable a la reingeniería procesal.

El funcionamiento del servicio de justicia en épocas de Covid-19 ha dado el puntapié inicial para el principio del fin del expediente soporte papel (COOKE, 2020).

Más allá de las loables repercusiones que esto pudiera tener en materia de sustentabilidad (disminución de la deforestación, emisión de CO2 y energía utilizada en el proceso de producción de papel), representa un “mojón” destacado en el camino a la justicia electrónica o *e-justice*.

La aplicación de las nuevas tecnologías no sólo en el ámbito de la gestión judicial sino también en la sustanciación del proceso, debe ser planteada como un objetivo necesario de cumplimentar para brindar un servicio acorde a las exigencias actuales.

En lo que a normativa respecta, numerosas disposiciones han surgido con posterioridad a la Acordada 4/2020 CSJN¹⁰³ que declaraba inhábil los días 16 a 31 de marzo de 2020.

Aquel conjunto de circunstancias excepcionales que convergió en la denominada “feria extraordinaria”, se transformó en la nueva normalidad.

Así, se debió prever la reactivación paulatina de uno de los servicios esenciales para el correcto funcionamiento del Estado de Derecho.

No obstante las dificultades estructurales y técnico-operativas que se evidenciaron

103 <https://www.cij.gov.ar/nota-36967-Acordada-4-2020-de-la-Corte-Suprema-de-Justicia-de-la-Nacion.html>

durante los primeros estadios de este proceso, resultaron tangibles las ventajas que traería esta nueva metodología tanto para operadores jurídicos como para justiciables, en términos de accesibilidad y celeridad.

Presenciamos, en este orden de ideas, un cambio sustancial en cuanto al ordenamiento procesal que presume de tener vocación de perpetuidad y que deberá ser receptado eventualmente por los códigos rituales a fin de brindar consonancia y consistencia entre lo normado y lo actuado.

CONCLUSIONES: ¿TEMPORALIDAD O SOSTENIBILIDAD?

Sin dudas, haber hecho frente al panorama de pandemia garantizando el acceso a la justicia es valorable. Sin embargo, recientes datos recolectados en relación al tópico “Covid-19 y Acceso a la Justicia” en la región iberoamericana, denotan que, en nuestro país, aún hay mucho por hacer.

Sobre la base de un cuestionario de seis ítems (**marco legal, normativa orgánica judicial, medidas gubernativas, medidas procesales, medidas de protección y apoyo al personal judicial y planes de futuro**) efectuado entre los países

pertenecientes a la región, se aprecian ámbitos a mejorar.

A efectos de no exceder el objeto del presente trabajo, no se ahondará en cuestiones de índole comparativa. Ello sería fútil y desalentador si, por ejemplo, evaluáramos nuestra *performance* buscando semejanzas con España, quien desde hace varios años se encuentra a la vanguardia de la implementación de la justicia electrónica.

Argentina, en tanto, fue destacada por la UNESCO en 2019 como uno de los cinco países de la región que ha avanzado en *alfabetización digital*.

No obstante, amerita un escueto análisis el acápite “**planes de futuro**” del instrumento antedicho (*Cumbre Judicial Iberoamericana, 2020*). En relación a aquél, Argentina optó por responder a tal punto “**en proceso de elaboración**”.

Se observa, claramente, la necesidad de **planificar** a efectos de sostener lo hasta aquí logrado y continuar su profundización.

Es dable decir que varias son las ventajas de la planificación: reduce la incertidumbre y los riesgos, genera motivación, tiene vocación de permanencia.

Tal vez planificar implique no comenzar a construir la casa por el tejado¹⁰⁴ (DÍAZ, 2020).

Estamos acostumbrados primeramente a normar, luego a implementar y por último a subsanar.

Mientras que por años defendimos la “justicia en formato papel”, pasamos súbitamente a constituimos en feligreses de la *e-justice*.

En medio de tal frenesí, se ubica la realidad.

Deberá el Estado, entonces -en conjunto con los operadores judiciales- abordar mediante políticas públicas serias y sostenibles en el tiempo, aspectos basales como el apoyo a las Provincias mediante financiación de inversiones para que factores relativos a accesibilidad, conectividad, estructuralidad y territorialidad, no trunquen la innovación tecnológica en el ámbito judicial.

Asimismo, configura un desafío para la Justicia estrechar lazos con la ciudadanía no sólo en contexto de urgencia.

Constituye para la Justicia, entonces, un imperativo ineludible e impostergable

adaptarse a un mundo contemporáneo en el cual el aprovechamiento e incorporación de los beneficios de las nuevas tecnologías en el modo de brindar servicios ha pasado a ser un estándar de calidad (JUSTICIA 2020, 2018).

En suma, en palabras de Albert Camus, **“todo lo que el hombre puede ganar al juego de la peste y de la vida es el conocimiento y el recuerdo”** (CAMUS, 1947).

BIBLIOGRAFÍA

- “Los 10 grandes desafíos a los que se enfrenta el mundo”, ETHICS.ES (2014). <https://ethic.es/>
- “La digitalización en el Poder Judicial: el anticipo de la despapelización definitiva” (p.2), Ezequiel Cooke (2020), SAIJ.
- “Informe de la Cumbre Judicial Iberoamericana” (p.86), Cumbre Judicial Iberoamericana, 2020.
- “Justicia 2020: cercana, moderna, transparente e independiente” (p.17), Programa Justicia 2020, www.bibliotecadigital.gov.ar, 2018.
- Díaz, María Fernanda. “La pandemia como precipitación necesaria de un nuevo ordenamiento judicial”, 3 Congreso Nacional de Derecho UNLPam, 2020.

104 DÍAZ, MARÍA FERNANDA. “La pandemia como precipitación necesaria de un nuevo ordenamiento judicial”, 3 Congreso Nacional de Derecho UNLPam, 2020.



- Camus, Albert. "La peste", Éditions Gallimard, 1947.



IMPLICANCIAS PRÁCTICAS DE LA RESOLUCIÓN 10/20 DICTADA POR EL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES EN EL RÉGIMEN DE NOTIFICACIONES¹⁰⁵

Julieta Melendi¹⁰⁶

RESUMEN

En la presente comunicación se analizarán las consecuencias prácticas de la Resolución 10/20 dictada por el presidente de la Suprema Corte de Justicia de la Provincia de Buenos Aires en el régimen de notificaciones. Si bien dicha Acordada fue dictada para regir en la emergencia, sus disposiciones propenden a la implementación plena del expediente digital en la provincia. Se abordarán los distintos medios de notificación utilizados en los casos en que la diligencia debiera ser cursada al domicilio real, es decir, los supuestos contemplados en el artículo 135 incisos 1°, 10 y 12 en los casos urgentes y en los no urgentes, destacando las controversias existentes respecto a la validez que tales actos de notificación entrañan y, a su vez, ponderaremos las ventajas que trae aparejada la notificación de la sentencia definitiva o aquella equiparable a esta por medios electrónicos, estimando de lege ferenda su incorporación en la ley de rito.

PALABRAS CLAVES: Carta Documento – WhatsApp –Nulidad- Sentencia definitiva

105 Enlace al video: <https://youtu.be/xgwozm6HsjE>

106 Instituto de Derecho Informático y TIC's del Colegio de Abogados y Procuradores de Bahía Blanca. Abogada, graduada en Universidad Nacional del Sur. Correo electrónico: julimelendi@gmail.com

I.- INTRODUCCIÓN

La Resolución 10/20 dictada por el Presidente de la SCBA¹⁰⁷ forma parte del plexo normativo dispuesto por la SCBA en la pandemia. Si bien posee carácter excepcional y transitorio, produjo diversas modificaciones en el Régimen de Notificaciones, tanto a la Acordada 3845/17¹⁰⁸ como al CPCPCBA. De conformidad con el régimen vigente en materia de notificaciones, solo deberán ser notificadas por cédula en formato papel las resoluciones que dispongan el traslado de la demanda, de la reconvenición y de los documentos que se acompañen con sus contestaciones; la citación de personas extrañas al proceso; y las sentencias definitivas o interlocutorias con fuerza de tales, con excepción de las que resuelvan negligencias en la producción de la prueba. El artículo 143 del CPCPCBA no admite como medio de notificación alternativo el correo electrónico oficial, el telegrama o la carta documento, en lo

107 Disponible en la web oficial de la SCBA: <http://www.scba.gov.ar/institucional/infoinstitucional.asp?date1=2020-3-18&date2=18%2F03%2F2020&expre=Resolucion+10%2F20&id=1&cat=0>

108 Disponible en la web oficial de la SCBA: <http://www.scba.gov.ar/servicios/notiypresen.asp>

supuestos previstos en el artículo 135 incisos 1º, 10 y 12 del CPCPCBA.

II.- DILIGENCIAS QUE DEBEN SER CURSADAS AL DOMICILIO REAL

Conforme a la Resolución 10/20 SCBA la cédula en formato papel queda relegada para aquellos casos en los que la diligencia deba ser cursada en el domicilio real. En los supuestos donde la diligencia reviste el carácter de urgente, la misma modifica la Acordada 3845/17, permitiendo que el organismo judicial remita en forma electrónica la cédula y la documentación a la oficina de Mandamientos y Notificaciones. Esta será la encargada de imprimir las copias para su posterior diligenciamiento y una vez efectuado, deberá escanear las constancias para su remisión al organismo judicial en forma electrónica.

Por otra parte, en aquellos casos donde la diligencia debe ser cursada al domicilio real y no reviste el carácter de urgente, los órganos judiciales de la provincia han optado por autorizar disímiles alternativas

para posibilitar el impulso procesal. Una de ellas es la empleada por algunos Tribunales de Trabajo permitiendo que el traslado de la demanda se efectúe por carta documento o telegrama, aplicando el artículo 16 de la Ley 11.653. A diferencia del artículo 143 CPCCBA, este artículo es suficientemente vasto y admite que todas las notificaciones que deban ser cursadas por cédula o personalmente se lleven a cabo no solo por los medios de notificación mencionados precedentemente, sino también por correo electrónico. En este sentido, el Tribunal de Trabajo N°2 de Morón¹⁰⁹, ordenó que el traslado de la demanda se efectúe por carta documento, haciendo saber al demandado que las copias de demanda y documental quedarían a disposición del interesado para su visualización en la Mesa de Entradas Virtual.

Otra alternativa fue la incorporación de la figura del oficial notificador ad hoc, aplicando en forma análoga la Acordada

109 "B. H. H. c/ Experta A.R.T. S.A. s/ enfermedad profesional", TTrab. N°2, Morón, 18/06/2020, Expte. N° 52.336, disponible en la web oficial del Colegio de Abogados de Morón, en: <https://camoron.org.ar/wp-content/uploads/2020/06/notificaci%C3%B3n-carta-documento-tribunal-2.pdf>

3397/08. Así, el letrado interviniente debe proponer a un abogado de la matrícula, quien efectuará la diligencia. Este último, debe presentarse en el expediente, aceptando el cargo y denunciando un domicilio electrónico al cual se le remitirán la cédula y la documentación para su posterior diligenciamiento. Una vez efectuado deberá escanear las constancias, y quedará como depositario de las originales.

Otra iniciativa fue la utilización de la plataforma WhatsApp. Cabe destacar que la Resolución 12/20 SCBA, establece que toda vez que en el fuero familia se reciban denuncias en casos de violencia familiar o de género, podrán utilizar dicha plataforma para comunicarse y notificar a las autoridades y a las partes, afirmando que tales actos gozan de plena validez. Si bien en los restantes fueros la SCBA no habilitó expresamente este medio de notificación, en el Convenio 526 celebrado entre la SCBA y la Asociación Judicial Bonaerense, se recomendó al personal judicial el empleo de las TIC's para la realización de actos internos y externos,

específicamente la utilización de medios telemáticos como WhatsApp para la comunicación de decisiones. En este sentido, el Juzgado de Paz de General La Madrid, ordenó que el traslado de la demanda de alimentos se lleve a cabo por WhatsApp. Sostuvo que debe flexibilizarse la normativa adjetiva teniendo en cuenta la situación que nos aqueja, garantizando la integridad de las partes como la de los oficiales notificadores. Destacó la importancia del interés superior del niño en materia de alimentos y consideró conveniente aplicar herramientas tecnológicas que garanticen la efectiva comunicación del acto y el derecho de defensa del demandado. En esta inteligencia, estableció recaudos para llevar a cabo la notificación. En principio, ordenó que el actuario descargue del sistema Augusta un PDF de las constancias obrantes en la causa, para luego comunicarse telefónicamente con el demandado, presentándose y solicitándole los datos que permitan su individualización. Posteriormente, informarle que se procedió a notificar la demanda a través de ese medio y que se

le remitirá el archivo PDF, comunicándole el plazo con el que cuenta para ejercer el derecho de defensa. Asimismo, resolvió que el actuario labre acta de lo acaecido, dejando constancia de la recepción del mensaje “si es que el demandado tiene activada dicha opción en la aplicación”¹¹⁰. Cabe destacar que no depende del usuario activar la opción para acreditar la recepción del mensaje, porque la misma opera automáticamente y se evidencia con la aparición de la doble tilde de color gris; en tanto que la doble tilde de color azul significa que el mensaje ha sido leído. La única opción con la que cuentan los usuarios es la de desactivar la doble tilde de color azul, con la finalidad de no evidenciar si los mensajes han sido leídos o no, en cuyo caso, aparecerá la doble tilde de color gris. Consideramos que para sustituir los medios establecidos por el CPCCBA y por la Resolución 10/20 SCBA (en el caso mediaba urgencia justificada en el mismo pronunciamiento) es necesario tener el conocimiento más acabado acerca del funcionamiento de

110 “S.S.G. c/ G.R.A. s/ alimentos” Juz. de Paz, Gral. San Martín, 02/04/2020, *elDial.com* - AAB1D.

estas plataformas. No obstante, el magistrado resolvió que eventualmente el actuario se comunique nuevamente por medio telefónico con el demandado a fin de verificar la recepción del mensaje.

La aquiescencia por parte de los órganos judiciales de efectuar la notificación mediante los medios analizados, conlleva la disyuntiva acerca de la validez que revisten tales actos. En un pronunciamiento, el Juzgado de Familia N° 7 de Morón, rechazó el pedido de nulidad de la notificación de alimentos provisorios efectuada por correo electrónico. El magistrado fundó el decisorio teniendo en cuenta la situación imperante, el DNU 297/20 y la Resolución 386/20 de la SCBA y sus prórrogas¹¹¹. Mencionó que el CPCBCA le confiere facultades instructorias para ordenar la notificación por dicho medio. Argumentó que el derecho en litigio se encuentra amparado por la Convención sobre los Derechos del niño, y goza de jerarquía constitucional¹¹².

111 Sucesión de Resoluciones de la SCBA desde el asueto judicial con suspensión de términos procesales hasta el progresivo restablecimiento del servicio de justicia: 386/20, 10/20, 15/20, 480/20, 558/20, 583/20, 593/20, 655/20, 3989/20 y 3991/20.

112 “R. D. V. M. M. c/ M. P. D. s/ alimentos”, Juz. Familia N° 7, Morón, 14/07/2020, Expte. N° 17.759,

En el contexto en el que nos encontramos inmersos, es necesaria la cooperación de todos los intervinientes, dejando de lado propósitos dilatorios u obstruccionistas. La declaración de nulidad del acto de notificación “debe responder a un fin práctico, resulta inconciliable con su índole de nulidad por la nulidad misma o para satisfacer un mero interés teórico”¹¹³. Coincidimos con Osvaldo A. Gozaíni (2003, 323) en que “si la finalidad del acto se cumple, y no hay perjuicios evidentes, no existirá estado de indefensión y, en consecuencia, no corresponderá admitir nulidad alguna”. Así lo sostuvo la SCBA afirmando que “(...) el resguardo de las formas procesales no puede, en principio, llevar al exceso ritual manifiesto”¹¹⁴, en tanto “(...) han sido creadas para garantizar los derechos de las partes y la buena marcha de las causas, pero no constituyen formalidades sacramentales

disponible en: http://e-procesal.com/notificacion-procesal-alimentos-provisorios-e-mail-nulidad-desestimacion-2471?fbclid=IwAR17Evlf6acvksV_FzP9qucGhYKKS4HbDPiB-LCSSagbHuNW4tCOdoLM-E.

113 CNCiv., Sala A, 08/09/1889, LL, t. 1989-E, p. 550.

114 “Mariani, Marta Elida c/Vieira Maia, Antonio s/Escrituración”, SCBA, 31/05/1994, Ac 49.959, disponible en la web oficial de la SCBA, en: <https://juba.scba.gov.ar/VerTextoCompleto.aspx?idFallo=111464>.

cuyo cumplimiento inexorable lleve implícita la sanción de nulidad”¹¹⁵. “Procurar la nulidad por la nulidad misma constituiría un ritualismo inadmisibles, que conspiraría contra el legítimo interés de las partes y la recta administración de justicia”¹¹⁶. Se debe garantizar la tutela judicial efectiva sin afectar el principio de contradicción y el derecho de defensa en juicio. Para calificar la nulidad del acto ha de tenerse en cuenta “si la notificación ha cumplido o no su finalidad propia; si ha causado perjuicio; si ha existido o no convalidación” (De Santo, 1999), con el fin de evitar que el impulso inicial del proceso, no se vea retrotraído en el caso de ser declarado nulo ulteriormente.

Con respecto a las sentencias definitivas o equiparables a ésta, que conforme a la normativa adjetiva deban ser notificadas en formato papel, la Resolución 10/20

115 “Torres, Osvaldo Raúl c/ Lemos y Rodríguez SA s/ Indemnización por enfermedad profesional”, SCBA, 18/06/2003, Ac. 77707, disponible en la web oficial de la SCBA, en: <https://juba.scba.gov.ar/VerTextoCompleto.aspx?idFallo=35748>.

116 “García, Adrián y otro c/Di Pascua, Marta L. y otro s/Daños y perjuicios”, SCBA, 13/09/2000, Ac. 72.490, disponible en la web oficial de la SCBA, en: <https://juba.scba.gov.ar/VerTextoCompleto.aspx?idFallo=59697>.

SCBA establece que deberán ser cursadas electrónicamente. Estimamos de lege ferenda que el CPCCBA debe incorporarlo. Se avizora que esta disposición coadyuva a la progresiva despapelización prevista en la Ley 25.506. Pensamos que la experiencia avala nuestra postura, ya que redundará en mayor celeridad y economía procesal. En esta inteligencia, concordamos con Carlos E. Camps (2020) en la utilidad de incorporar al sistema de gestión un mecanismo que posibilite la “notificación electrónica automática”, esto es, que “en el mismo momento que el juez firma una resolución, ésta sea registrada digitalmente y notificada electrónicamente a los interesados”, generando mayor eficacia procesal al posibilitar que la firma del resolutorio y el libramiento de la cédula se produzcan en simultáneo. A mayor abundamiento, Gastón E. Bielli y Andrés L. Nizzo (2017) destacan que uno de los beneficios que trae aparejada la notificación electrónica es la certeza que otorga a los profesionales intervinientes en tanto trae ínsito un “cuádruple control”. El mismo es conferido por el mail de cortesía, por la solapa de notificaciones del Portal

de Notificaciones y Presentaciones Electrónicas, por el mail proveniente de la Mesa de Entradas Virtual, y por la propia Mesa de Entradas Virtual cuando ingresamos en la causa. Asimismo, teniendo en cuenta que el Reglamento aprobado por la Acordada 3975/20 SCBA, sienta como regla que todas las resoluciones y sentencias se generen y rubriquen digitalmente y, que los expedientes tramiten en formato digital, consideramos que para armonizar dicha normativa con la vigente lo más apropiado es llevar a cabo la reforma que proponemos.

III.- REFLEXIONES FINALES

La Resolución 10/20 SCBA, constituye un verdadero reglamento que impone pautas de actuación a los intervinientes en el proceso (Nizzo y Rosales Cuello, 2020). En lo que nos atañe, ha venido a incorporar modificaciones de gran utilidad. Entre ellas, en los supuestos en que la diligencia revista carácter de urgente y deba cursarse en un domicilio real, se permite la remisión por medios

electrónicos de las cédulas y de la documentación por parte de los organismos judiciales a la oficina de Mandamientos y Notificaciones, y por parte de ésta a aquellos de las constancias resultantes luego de efectuado el diligenciamiento. Es destacable la labor de los organismos judiciales que pese a las limitaciones existentes permitieron impulsar el proceso autorizando medios alternativos de notificación. Se deberá analizar en cada caso el justo medio que garantice el principio de bilateralidad, el derecho de defensa en juicio y, a su vez, ponderar si el acto de comunicación cumple con el fin previsto, si genera un daño y si tal acto es subsanado, para posibilitar que la tutela judicial sea efectiva.

Otra modificación que introdujo la Resolución 10/20 SCBA, es la notificación por medios electrónicos de la sentencia definitiva o de aquella equiparable a ésta. Estimamos de lege ferenda que tal disposición debe ser incorporada en la ley de rito por las ventajas que trae aparejada. Esto es, propende a la progresiva despapelización generando mayor

economía y celeridad procesal, y acrecienta la certeza en sus destinatarios, quienes podrán ejercer un cuádruple control sobre el acto de notificación.

BIBLIOGRAFÍA

- BIELLI, Gastón E. y NIZZO, Andrés L. (2017), “Domicilio electrónico y notificaciones electrónicas. El aspecto más beneficioso del portal SNPE”, IADPI, marzo. Disponible en: <https://iadpi.com.ar/2017/03/28/domicilio-electronico-y-notificaciones-electronicas/>.
- CAMPS, Carlos E. (2020), “Eficacia del derecho procesal electrónico bonaerense y

pandemia”, LLBA, mayo, p.3, AR/DOC/1525/2020.

- DE SANTO, Víctor (1999), Nulidades procesales, Buenos Aires, Ed. Universidad, p. 113.
- GOZAÍNI, Osvaldo A. (2003), “Código Procesal Civil y Comercial de la Provincia de Buenos Aires: comentado y anotado”, t.1, 1° edición, Buenos Aires, Ed. La Ley, p. 323.
- NIZZO, Andrés L. y ROSALES CUELLO, Ramiro (2020), “La prestación del servicio de justicia bonaerense durante el estado de emergencia sanitaria”, junio, elDial.com - DC2B44, p. 2.

EL SISTEMA DE UDRP DE ICANN APLICADO COMO MODELO A CONFLICTOS DE COMERCIO ELECTRÓNICO¹¹⁷

Rolando Joaquín Ortega Hernández¹¹⁸

RESUMEN

El sistema de la UDRP de ICANN es un procedimiento de ODR sobre resolución de conflictos entre legítimos propietarios de signos distintivos y registrantes de nombres de dominio. Este procedimiento con muchas semejanzas al arbitraje ha logrado reducir enormemente la conflictividad entre legítimos propietarios de nombres de dominio y ciber ocupas. Se trata de un procedimiento autorregulado y no excluyente de la jurisdicción ordinaria ni del arbitraje.

El propósito de este trabajo es plantear la posibilidad de utilizar el procedimiento de la UDRP de ICANN para el comercio electrónico en general como referente, con obvias modificaciones. Igualmente plantear la posibilidad de implantar un sistema híbrido, del tipo autocompositivo y hetero-compositivo, de carácter obligatorio, pero no excluyente de la jurisdicción ordinaria ni antes, ni durante ni después de iniciado el conflicto al igual que el procedimiento de la UDRP.

Palabras Clave. UDRP, ICANN, ODR, Arbitraje.

117 Enlace al video: <https://youtu.be/OZ2fw4YYWBQ>

118 Profesor Universidad Internacional de la Rioja - Doctorado Universidad de Salamanca - Abogado Universidad Santa María (Venezuela), homologado en U.de Salamanca y en la Universidad NLP (Argentina).
mail: rolandortega@hotmail.com

INTRODUCCIÓN

El procedimiento administrativo obligatorio de la *Uniform Dispute Resolution Policy* (UDRP) de la *Internet Commission for Assigned Names and Numbers* (ICANN)¹¹⁹ ha constituido un hito en los procedimientos de ODR. Constituye un procedimiento *sui-generis* que ha dado respuesta a la conflictividad entre legítimos propietarios de nombres de dominio y signos distintivos. Mediante la aplicación de este procedimiento se ha logrado encausar la enorme problemática universal sobre registros abusivos de nombres de dominio a tres parámetros concurrentes. Dichos parámetros o causales son: (i) *que su nombre de dominio es idéntico, o similar hasta el punto de poderlo confundir, a una marca de productos o de servicios sobre los cuales el demandante tiene derechos;* (ii) *que usted no tiene derechos o intereses legítimos con respecto al nombre de dominio;*(iii) *que su nombre de dominio ha*

¹¹⁹ la Corporación de Internet para Nombres y Números Asignados (ICANN) coordina las funciones de *Internet Assigned Numbers Authority* (IANA), que son los servicios técnicos críticos clave para las operaciones continuadas de la libreta de direcciones subyacente de Internet y el sistema de nombres de dominio (DNS). ICANN realiza las funciones de IANA en virtud de un contrato con el Gobierno EE.UU..

sido registrado y está siendo utilizado de mala fe (Art.4.a de la UDRP).

El propósito de esta comunicación es exponer la posibilidad de aplicar a manera de referencia y con los cambios oportunos, un sistema similar al de la UDRP para el comercio electrónico B2C. Esta idea está motivada por las discrepancias doctrinales y legales en cuanto a la implementación de un sistema arbitral para el comercio electrónico transfronterizo, precedido de un procedimiento consensual o si por el contrario se aplicaría un procedimiento de mediación tradicional. No es pacífica la doctrina a nivel internacional en cuanto a la aceptación de una cláusula arbitral *ex ante* cuando la parte contratante es un consumidor. El procedimiento de UDRP de ICANN no entra a valorar la legalidad de implementar una cláusula de resolución de conflictos, de forma obligatoria y de adhesión, ya que se trata de un procedimiento de naturaleza privada que no excluye acciones particulares del conocimiento de los tribunales ordinarios ni antes ni después de iniciado el procedimiento.

Por otra parte, existe a nivel regulatorio internacional la necesidad de implementar un modelo efectivo y que satisfaga las

necesidades del mercado y que al mismo tiempo no menoscabe los derechos del consumidor como débil jurídico. Estos incrementos regulatorios, buscan brindar un marco regulatorio para armonizar los criterios de resolución alternativa de conflictos en el comercio electrónico B2B y B2C. A nivel Europeo, tenemos dos instrumentos normativos de derecho positivo: 1) La Directiva 2013/11/UE del Parlamento Europeo y Del Consejo de 21 de mayo de 2013 relativa a la resolución alternativa de litigios en materia de consumo (Directiva sobre resolución alternativa de litigios en materia de consumo) (DRALC) y; 2) el Reglamento (UE) No 524/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 sobre resolución de litigios en línea en materia de consumo o Reglamento Europeo de Resolución de Litigios en Línea (RERLL). Por otra parte, y con un carácter supletorio o como un instrumento del *Soft Law*, se encuentran los documentos del grupo de trabajo III de UNCITRAL/CNUDMI de las naciones unidas sobre solución de controversias en línea. Todos estos instrumentos pueden ser adaptados a un procedimiento similar a la UDRP de ICANN de forma autorregulada y unificada a nivel mundial.

CONTENIDO

Sobre la naturaleza jurídica de la UDRP de ICANN habría que decir que, la UDRP de ICANN tiene carácter universal y obligatorio para los solicitantes de gTLDs¹²⁰ abiertos. De esta manera, quien solicita el registro de un SLD¹²¹ bajo la modalidad de gTLD abierto queda automáticamente obligado contractualmente a someterse a ese procedimiento al celebrar un contrato de registro con cualquiera de los registradores acreditados de la ICANN; dicho contrato conlleva la aceptación de una cláusula de adhesión de sometimiento al procedimiento administrativo obligatorio de resolución de controversias entre los solicitantes de nombres de dominio gTLDs abiertos y los legítimos propietarios de signos distintivos.

La entidad encargada acreditada por ICANN para la resolución de los conflictos, es una institución

120 El acrónimo gTLD abierto hace referencia al *Top Level Domain* que es el dominio de primer nivel. Es la categoría mas alta del sistema de nombres de dominio de carácter abierto e internacional de ICANN. Ej. “.com”, “.org”, “.edu”, “.mil”, “.gov”, “.net”.

121 El acrónimo SLD hace referencia al dominio de segundo nivel (Second Level Domain), es la parte mas visible del nombre de dominio y que puede presentar mas confusión a los usuarios. Ej. En el dominio <http://www.usal.es> , la palabra “usal” sería el SLD.

independiente y separada de la entidad encargada del registro del SLD para así garantizar la independencia de la solución. Estos proveedores de servicios son instituciones privadas, que generalmente prestan servicios de mediación y arbitraje privados, como el Centro de Mediación y Arbitraje de la OMPI. Así, un demandante, sabedor de su mejor derecho sobre el dominio registrado deberá seleccionar a un proveedor de servicios de ODR acreditados por ICANN bajo la modalidad de UDRP. Por lo que, el registrador no tendrá participación de ninguna manera en la controversia que surja entre el demandante y otra parte distinta a la del registrador en referencia al registro y utilización del nombre de dominio en conflicto. Las entidades acreditadas por ICANN bajo la política uniforme de la UDRP son actualmente: [Asian Domain Name Dispute Resolution Centre](http://www.adndrc.org/mten/index.php)¹²² (ADNDRC), [National Arbitration Forum](http://www.adrforum.com/Home/HomePage)¹²³ (NAF), El centro de Mediación y Arbitraje de la OMPI¹²⁴, [The Czech Arbitration Court Arbitration Center for Internet](http://www.wipo.int/amc/es/domains/)

122 Información disponible en: <http://www.adndrc.org/mten/index.php> (Última visita, 24-06-2016)

123 Información disponible en: <http://www.adrforum.com/Home/HomePage> (Última visita, 24-06-2016)

124 Información disponible en: <http://www.wipo.int/amc/es/domains/> (Última visita, 24-06-2016)

[Disputes](#)¹²⁵ (CAC) y el [Arab Center for Domain Name Dispute Resolution \(ACDR\)](#)¹²⁶.

La UDRP no es un Arbitraje. En ocasiones, la doctrina generalizada de ODR ha confundido el procedimiento utilizado en la UDRP con el Arbitraje. Tal confusión deriva de la errónea alusión a los integrantes de los paneles de expertos dentro de la redacción del documento y el reglamento de la UDRP como “árbitros”¹²⁷, a tal punto que se le ha calificado como un proceso *cuasi arbitral*. En efecto, existe cierta proximidad con el arbitraje, ya que es un procedimiento extrajudicial heterocompositivo de resolución de controversias y su aceptación deriva de un contrato, similar al convenio arbitral, sin embargo, consideramos necesario precisar que no es un arbitraje.

Ahora bien, debemos plantearnos la posibilidad de utilizar la UDRP de ICANN para los conflictos derivados del comercio electrónico B2B y B2C. Debemos señalar que la implantación de un sistema global transfronterizo de resolución de conflictos para el comercio electrónico B2C no debe excluir el acceso a la jurisdicción de los

125 Información disponible en: <http://www.adr.eu/> (Última visita, 24-06-2016)

126 Información disponible en: <http://acdr.aipmas.org/?lang=en> (Última visita, 17-05-2015)

127 Vid. OMPI D.2000-0910 casos «portaventura.net» y «portaventura.org».

tribunales ordinarios. De hecho, a pesar del marcado carácter arbitral de la UDRP de ICANN este sistema no impide a ninguna de las partes acudir a la jurisdicción ordinaria en caso de que deseen entablar una acción ante la jurisdicción ordinaria, como si ocurre en el arbitraje debido a su efecto negativo de exclusión del conocimiento del asunto a los tribunales ordinarios. Esta situación es necesario evaluarla si se quiere implantar un sistema de ODR para el comercio electrónico B2C, para no vulnerar el derecho a la tutela judicial efectiva ni ningún otro derecho derivado de la suscripción de un convenio arbitral en una cláusula de adhesión, como la posibilidad de que los consumidores acudan en forma colectiva a hacer valer sus derechos mediante acciones de clase.

CONCLUSIONES

El procedimiento de la UDRP de ICANN constituye un hito en la doctrina de los ODR. Debido a su adaptación al entorno de la Sociedad de la Información y a que ha producido unos resultados bastante positivos en cuanto a la reducción y creación de parámetros para resolver conflictos entre legítimos

propietarios de marcas de productos y servicios.

El comercio electrónico B2B y B2C demanda la creación de un sistema de ODR global y unificado. Este sistema solo será posible con el esfuerzo y el consenso de los principales actores del mercado a través de la creación de un modelo unificado, cumplimentado por un sello de confianza internacional. Igualmente el sistema debe formarse en base a un modelo integrado en etapas o fases del conflicto, una etapa autocompositiva donde los métodos consensuales como la mediación o negociación asistida y automatizada tengan cabida, seguido de una etapa adversarial dirigida por un tercero neutral quien emitirá una decisión, ejecutable desde el punto de vista privado y del mercado pero que no excluya a las partes de la posibilidad de ejercicio de acciones judiciales, bien sea de forma individual como en forma colectiva.

Por estas razones, debido al éxito de la UDRP como un *tertium genus* entre el arbitraje y otros métodos heterocompositivos es que se propone tomar a la UDRP como modelo referente para la creación de un sistema global transfronterizo de ODR para el comercio electrónico B2B y B2C. Ya que es un sistema autorregulado y no menoscaba

los derechos del ejercicio de la tutela judicial efectiva. La adaptación al entorno de los principios de los métodos extrajudiciales de resolución de conflictos y el no caer en la tentación de extrapolar al pie de la letra métodos como el arbitraje que a pesar de sus beneficios se han dado en contextos históricos de otras peculiaridades que el comercio electrónico transfronterizo, fue uno de los éxitos de la UDRP. Debemos recorrer un camino parecido para la resolución de conflictos derivados del comercio electrónico en internet.

BIBLIOGRAFÍA

- AGUSTINOY GUILAYN, Albert. Nombres de Dominio. Normativa Internacional, Comunitaria y Española Comentada. Ed: Bosh. Barcelona, 2008
- ALPANA, Roy. "Reflections On The Uniform Domain Name Dispute Resolution Policy As It Enters Its Second Decade". *Int. J. Technology Policy and Law*, Vol. 1, No. 1, 2012. Pp. 15-24
- ANDERSON, Edward C. COLE, Timothy S. "The UDRP – A Model for Dispute Resolution in E-Commerce?" *The Journal of Small and Emerging Business Law*. Vol.6. N0.235. Año 2002
- BOWER, Michael G. "Implementing an Online Dispute Resolution Scheme: Using Domain Name Registration Contracts to Create a Workable Framework". *Vanderbilt Law Review*. Vol. 64. No.4, Mayo 2011. Pp.1265-1309.
- CARBAJO CASCÓN, Fernando. Conflictos entre Signos Distintivos y Nombres de Dominio en Internet. Ed. Aranzadi, 2ª ed. Navarra, 2002
- CARBAJO CASCÓN, Fernando. Nombres de Dominio de Internet. Cap.7. P.441. En: AAVV ORDUÑA, Javier. AGUILERA, Gonzalo (Dir.) PLAZA, Javier. BALLUGERA, Carlos (Coords.) Comercio, Administración y Registros Electrónicos. Ed: Aranzadi. Navarra, 2009
- CHATTERJEE, Nilanjana. "Arbitration Proceedings Under ICANN'S Uniform Domain Name Dispute Resolution Policy- A Myth or Reality?". *RDA/BLJ*. N°5. 2006. Pp.728-737
- CHRISTIE, Andrew. "The ICANN Domain-Name Dispute Resolution System as a Model for Resolving Intellectual Property Disputes on the Internet". *The Journal of World Intellectual Property*".Vol. 5, Suplemento 1. 2005
- CORTÉS DIEGUEZ, Juan P. "Domain Names And The Uniform Dispute Resolution Policy an Analysis Of The UDRP Experience – Is it time for reform?". *Computer law & security report* . Vol. 24. Año (2008). Pp. 349-359
- DONAHEY, Scott M. "The UDRP Model Applied to Online Consumer Transactions". *Journal of International Arbitration*. Vol. 20. No.5, 2003. Pp.475-491
- DONAHEY, Scott M. "The Uniform Domain Name Dispute Resolution Process and the Appearance of Partiality. Panelists Impaled on the Horns of a Dilema." *Journal of International Arbitration*. Vol. 19. No.1. 2002. Pp.33-38
- KATSH, Ethan, y RIFKIN, Janet. : *Online Dispute Resolution: Resolving Conflicts in Cyberspace*. Ed: Jossey-Bass. San Francisco, E.U.A., 2001
- MILLER, Kimberly J. "The Uniform Dispute Resolution Policy: An Uphill Fight for Domain Name Registrants" *The Journal of Contemporary Legal Issues*. Vol. 19: 520, 2010. Pp. 520-529
- BOWER, Michael G. "Implementing an Online Dispute Resolution Scheme: Using Domain Name Registration Contracts to Create a Workable Framework". *Vanderbilt Law*



Review. Vol. 64. No.4, Mayo 2011. Pp.1265-1309

RABINOVICH-EINY, Orna. KATSH, Ethan. "Technology and the Future of Dispute Systems Design" *Harvard Negotiation Law Review*. Vol.17. Nº 151, 2012. Pp. 151-199

VALLÉS BOTEY, Martí. "El Proceso Cuasi-Arbitral en Conflictos Relativos a Nombres de Dominio". *Anuario de Justicia Alternativa*. Núm 2, 2002. Pp.51-61



CRÓNICA DE UN RECHAZO ANUNCIADO, A Propósito del Per Saltum de Google¹²⁸

Mariel Alejandra Suárez¹²⁹

RESUMEN

La Corte Suprema de la Nación Argentina, ha rechazado un per saltum presentado por el gigante digital Google, en virtud de que en primera instancia se hizo lugar una medida cautelar, imponiendo la aplicación del Instituto denominado Prueba Anticipada, en virtud del reclamo de la Vice Presidenta de la Nación, quien peticionó ingresar al sistema informático de la empresa y hacerse de los elementos probatorios para entablar en un futuro, una demanda en su contra.

Que la situación tuvo su origen belicoso, cuando en el buscador de la empresa aparecía su nombre asociado al mote de "ladrona de la Nación Argentina", exactamente en el panel de conocimiento de la página.

El presente trabajo invita a analizar los argumentos usados por las partes y por el juez al dictar la resolución, como también, a verificar si el instituto que es de aplicación excepcional, corre el riesgo de convertirse en la regla a aplicar, siempre que haya que obtener evidencia digital.

128 Enlace al video https://youtu.be/6lsW6wO_VhQ

129 Jueza Penal Chubut – Argentina, Experta en Cibercrimen, Ciberseguridad, Protección de datos y Derechos Digitales. Mail masuarez@juschubut.gov.ar ;

Palabras claves: evidencia digital – prueba anticipada – demanda – medida cautela – google – panel de conocimiento

INTRODUCCIÓN

Se explicará en forma breve, como el caso no debió encuadrarse en el marco del instituto de la Prueba Anticipada y, que la especialidad y especificidad del tipo de evidencia que es la digital, no los autorizaba a su aplicación, pues existen otros remedios tan o más eficaces que el instituto aplicado, los que además son los pertinentes.

Que es cierto que la evidencia digital tiene especiales características, pero que esas características no autorizan a echar mano a institutos de excepción, con el riesgo de que se conviertan en generales.

DE LA EVIDENCIA DIGITAL Y SU TRATAMIENTO

Resulta imprescindible definir el concepto de evidencia digital y referirnos a su tratamiento.

Puede decirse que es cualquier tipo de información creada, almacenada, o transmitida en forma digital, la que esta conformada por dígitos, los que finalmente generalmente se representa en

una imagen estática, un mensaje de audio y video o de texto, pero que esa representación no es la evidencia en sí.

La evidencia, justamente, es lo que está detrás de lo que vemos. Aquellos metadatos, esa información que nos puede revelar la IP del posible autor, su geolocalización, el peso del archivo, entre otros datos, impulsos electrónicos que nos indican que eso que aquello que vemos, existió en el universo digital. Los Códigos Procesales, nada dicen al respecto. Enuncian reglas generales en materia probatoria en consonancia con las Constituciones.

La utilidad actual de la evidencia digital, es indiscutible, prueba delitos comunes tanto como los específicamente informáticos, y puede ser usada tanto en procesos civiles, laborales o administrativos a favor o en contra de una pretensión.

Para el levantamiento de cualquier tipo de rastros, existen protocolos en el ámbito de la Justicia, el cuerpo policial o las Fiscalías.

Si se carecen de ellos, en materia de evidencia digital, existen reglas y

protocolos internacionales estandarizados que pueden ser de efectiva aplicación como la RFC 3227¹³⁰ del año 2002 o la norma ISO 27037¹³¹ del año 2012 entre otras, o los protocolos o manuales del INCIBE¹³² o de la OEA¹³³, no se contraponen con las legislaciones procesales y respetan garantías constitucionales y convencionales, posibilitando control ulterior, para lo que ha de intervenir un Perito Informático Forense.

DEL TRABAJO DE LOS PERITOS INFORMÁTICOS FORENSES Y LA PRESENTACIÓN DE LA EVIDENCIA DIGITAL ANTE EL JUEZ

Las normas procesales, en el mundo, no distinguen las facultades u obligaciones de éstos peritos, de los informáticos del resto de los peritos. con el resto, Tampoco se les exige una profesión

130 RFC “Request For Comments” <https://www.rfc-es.org/pendientes/rfc3227-es.nroff> consultada el 10/10/2020

131 <https://www.iso.org/standard/44381.html> consultada el 13/10/2020

132 INCIBE (Instituto de Ciberseguridad Español) <https://www.incibe.es/protege-tu-empresa/guias> consultada el 13/10/2020

133 OEA (Organización de los Estados Americanos) https://www.oas.org/juridico/english/cyb_pan_m_anual.pdf consultada el 14/10/2020

específica, pudiendo ser abogados expertos, ingenieros o licenciados en informática.

No hay uniformidad a la hora de saber si deben colegiarse o no para ejercer su profesión, pero a nivel internacional ya existen Asociaciones de Peritos Informáticos¹³⁴, que prestigian la actividad, fomentando la interdisciplinariedad y la capacitación.

El perito informático es aquél profesional experto, capacitado para hacer la extracción de la evidencia digital, en forma previa o durante la tramitación de un proceso judicial.

La experticia del mismo, está sujeta a reglas procesales que determinan que su actividad debe llevarse con objetividad, diligencia, y buena fe.

Luego de hacer la experticia, esta obligado a prestar juramento, como cualquier otro perito de parte o testigo.

La oportunidad de realizar su tarea, será conforme al nivel de volatilidad de la evidencia y las necesidades de quien lo contrata y, lo hará mediante un informe, el que se ofrecerá como prueba documental

134 <https://www.aspei.es/> consultada el 13/10/2020; y la APPIF Panamá, Asociación de Peritos Informáticos Panamá <https://www.facebook.com/appifpanama/> consultada el 13/10/2020

y los elementos sobre los que realiza su experticia deben estar ofrecidos como elementos secuestrados, dejando la posibilidad a que otros peritos controlen su trabajo o realicen uno nuevo.

En la etapa de la producción de la prueba es que será citado a declarar bajo juramento, oportunidad en que las partes podrán realizar preguntas y contra preguntas para examinar al mismo, el que declarara bajo juramento.

El perito no suple la tarea del Juez, es un auxiliar. Habrá quienes dirán que todo va a girar en torno al resultado de la pericia, pero lo cierto es que una única prueba no es la que define el resultado de un proceso, sino el análisis en su conjunto, con el resto de los elementos probatorios ofrecidos y reproducidos en la etapa pertinente.

Por eso, su función es trascendente en todo tipo de procesos en los que haya que coleccionar evidencia digital.

A PROPÓSITO DEL CASO GOOGLE – ALGUNAS REFERENCIAS SOBRE LA PRUEBA ANTICIPADA

Hechas estas aclaraciones necesarias, el caso analizado, tuvo inicio cuando una persona pública, se sintió afectada por un

comentario que apareció sobre su persona en el panel de conocimiento del conocido buscador de google.

Esa información en el panel de conocimiento, apareció el mote especificado, encabezado por una información que fue proporcionada por el sitio de “*Wikipedia*”, una enciclopedia pública en la que cualquiera persona puede colaborar aportando información.

Es de destacar, que no se verificó si tal información aparecía en otros buscadores, como tampoco cual es el motivo, que lleva a que los resultados de la enciclopedia, se posicionen mejor que otros resultados.¹³⁵

Los reclamantes, tampoco se percataron que Wikipedia no es Google y que quien proveía de esa información no era el buscador sino la enciclopedia.¹³⁶

Cabe señalar que, algunos buscadores poseen la función de panel de conocimiento y otros no. Se trata de una especie de resumen destacado, que según google¹³⁷ se genera

135 <https://rockcontent.com/es/blog/wikipedia-tope-de-las-busquedas> consultada el 13/10/2020; https://es.wikipedia.org/wiki/Posicionamiento_en_buscadores consultada el 13/10/2020

136 <https://www.lanacion.com.ar/tecnologia/como-llego-cristina-kirchner-figurar-como-ladrona-nid2414162> consultada el 13/10/2020.

137 <https://support.google.com/knowledgepanel/answer/9163198?hl=es-419> consultada el

automáticamente en casos de cierta importancia pública de la información buscada.

La accionante, Se requirió entonces, que como medida previa se autorice la aplicación del instituto de **anticipo de prueba** con el objeto de extraer datos referidos a la publicación, basando su petición en razón de en que el que el posible demandado, quien es el que quién administra las base de datos de donde surge dicha información, pudiera alterarla o incluso hacerla desaparecer con lo cual la información corría peligro de desaparecer.

Es de destacar, que el buscador, en éste caso, demoro tardo menos de 24 horas s de para proceder a la supresión de la misma, cuando en otros casos hasta se ha requerido la intervención judicial y la supresión de la información ha llegado años después, generando una especie de discrecionalidad en el accionar de la empresa, lo que vale la pena señalar, pero que no es motivo de análisis del presente trabajo.¹³⁸

Ahora bien, el instituto de la Prueba Anticipada es de excepción, dado que la producción de la prueba en un proceso,

12/10/2020.

138 CSJN, R. 522. XLIX, "Rodríguez, Maria Belén c/ Google Inc. s/daños y perjuicios", 28 de octubre de 2014.

cualquiera sea el tipo, se reserva para la etapa específica, de debate, oportunidad en la que el demandado o denunciado, pueda defenderse contradiciendo la pretensión de la demandante o denunciante, controlando la prueba, en resguardo de las garantías constitucionales y convencionales.¹³⁹

En primera instancia y basado en la característica principal de la evidencia digital, o sea la volatilidad, se le concedió a la actora la aplicación del referido instituto, permitiéndole que previo a iniciar

139 Art. 326 del CPPCyC de la Nación “.....los que sean o vayan a ser parte en un proceso de conocimiento y tuvieren motivos justificados para temer que la producción de sus pruebas pudiera resultar imposible o muy dificultosa en el período de prueba....” Lo que también se contempla en Procedimientos Penales a modo de ejemplo **art. 279 CPPCH**”....Las partes podrán solicitar, fundadamente, el anticipo jurisdiccional de prueba en los siguientes casos: 1) cuando se tratara de un acto que, por las circunstancias o por la naturaleza y características de la medida, deba ser considerado como un acto definitivo e irreproducible; 2) cuando se tratara de una declaración que por un obstáculo difícil de superar fuere probable que no pudiera recibirse durante el juicio; 3) cuando por la complejidad del asunto existiera la probabilidad de que el testigo olvidare circunstancias esenciales sobre lo que ha conocido; 4) cuando el imputado estuviere prófugo, fuere incapaz o existiere un obstáculo constitucional y se temiera que el transcurso del tiempo dificultara la conservación de la prueba....” Consultado en https://leyes-ar.com/codigo_procesal_penal_chubut/279.htm el 13/10/2020

un planteo de fondo, extraiga la evidencia digital de la empresa.

Por su parte, Google, el gigante digital impugnó la concesión de la medida, con fundamento en la sensibilidad de los datos que la mencionada empresa maneja y el potencial peligro que significaría que la reclamante, ingrese a sus sistema informático.

El recurso fue rechazado e impetro lo que le fue rechazado para finalmente, interponer el Per Saltum motivado en los argumentos señalados, centralmente en la calidad y cantidad sensibilidad dde los datos que contiene la plataforma, sobre millones de personas y que el acceso a la misma podría exponer a terceros que nada tienen que ver en el pleito, lo que nuevamente fuera desestimado.

Ni la actora, ni la demandada, ni el Juez, advirtieron que esto no se trata del manejo de datos sensibles por ejemplo, porque en el caso de que los haya y exista un reclamo judicial, con las debidas precauciones un especialista (perito informático) puede operar pericialmente sobre los mismos.

Tampoco advirtieron que la volatilidad de la evidencia digital, no justifica la aplicación del instituto de prueba anticipada, dado que existen múltiples

opciones para poder realizar la extracción y preservación de la prueba, aun en el caso de que desaparezca, y que la prueba digital es la prueba esencial en el caso, pero no la única, dado que también se puede ofrecer prueba de informes por ejemplo.

DE LOS ANÁLISIS QUE NO SE EFECTUARON A MODO DE CONCLUSIÓN:

Para ir concluyendo y completar el análisis crítico, resulta necesario resaltar las cuestiones que las partes no tuvieron en cuenta al momento de entablar el reclamo, contestarlo o resolverlo.

Primero, la esencia de la evidencia digital y el tipo de evidencia que se pretendía manipular.

No consideraron que la evidencia consistía en metadata que proporcionaba una página web con determinada información o contenido, que había sido replicado al menos por un buscador, el posible demandado.

No advirtieron justamente esta circunstancia central, que la información estaba siendo publicada por otro sitio.

Que se podrían haber efectuado pericias sobre la página por ejemplo desde la computadora del demandante o

damnificado mediante la intervención de un perito forense de parte, quien conforme los protocolos referenciados, pudo asegurar el contenido del link, posibilitando un control posterior, por ejemplo sellando la actividad y encriptándola con un hash, lo que incluso pudo asegurarse mediante un testigo online¹⁴⁰.

Que se pudieron haber obtenido las IP del particular que posteo el comentario infructuoso en la enciclopedia pública.

Que la intervención Judicial, pudo haber sido al solo efecto de librar un oficio tendiente a preservar o congelar la información.

Al momento de interponer el Per Saltum, no se consideraron como argumentos de la interposición, que la propia demanda, no sería la que manipularía la información en forma personal, sino un perito judicial, quien operaría en forma remota y no en forma directa desde el ordenador de la empresa.

Nadie tuvo en cuenta, la excepcionalidad del instituto de la Prueba Anticipada, ni el riesgo de que se convierta en regla, en los casos en que haya evidencia digital para recolectar, o sea, la mayoría de los casos.

140 <https://www.incibe.es/protege-tu-empresa/blog/recoleccion-pruebas-digitales-testigos-online> consultada el 14/10/2020

No considerar estas cuestiones llevaron a las partes a plantear lo que plantearon y a quienes resolvieron, a resolver como lo hicieron, dejando un riesgo latente, que es que la excepción se convierta en regla.

BIBLIOGRAFÍA

- Código Procesal Penal de la Nación
- Código Procesal Civil y Comercial de la Nación
- Constitución Nacional
- Gaston Semprini "Estandarización de procedimientos y protocolos del laboratorio de Informática Forense". SID 2015. Anuales 44 JAIIO – Jornadas Argentinas de Informática – Rosario
- Cano, Jeimy. Computación Forense. Descubriendo los Rastros Informáticos. Alfaomega. Méjico. (2009)
- <https://www.tech4law.co.za/tech-advisor/107-digital-forensics/1528-what-is-digital-forensics>.
- Olivier, Martin S. (March 2009). "On metadata context in Database Forensics" 8. Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. <http://www.pensamientopenal.com.ar/sistem/files/2016/05/doctrina43429.pdf>
- RFC "Request For Comments" <https://www.rfc-es.org/pendientes/rfc3227-es.nroff> consultada el 10/10/2020
- NORMA ISO 27037 <https://www.iso.org/standard/44381.html> consultada el 13/10/2020
- Nota periodística <https://www.lanacion.com.ar/tecnologia/como-llego-cristina-kirchner-figurar-como-ladrona-nid2414162> consultada el 13/10/2020.

- Davara Rodríguez, M. (2001). Manual de derecho informático. (3ª ed.) Pamplona, España: Arazandi.
- Rico Carrillo, M. (2007). *Derecho de las nuevas tecnologías*. Buenos Aires:

LA PRUEBA EN LAS OPERACIONES CON CRIPTOACTIVOS¹⁴¹

Fernando O. Branciforte¹⁴²

RESUMEN

En la realidad económica actual, las operaciones con criptoactivos se encuentran a la orden del día y se han masificado y adquirido una gran popularidad en nuestro país y en el mundo.

Con dicha masificación y popularidad también comienzan a aparecer los conflictos en las distintas relaciones jurídicas que se realizan con ellas.

A veces por el desconocimiento en el sistema, otras por el aprovechamiento de algunos, lo cierto es que de una u otra manera, determinados usuarios de estos “nuevos sistemas” salen perjudicados en sus derechos y en su patrimonio.

La intención del presente trabajo es analizar, de forma muy abreviada, esas situaciones y qué elementos contaríamos para utilizar como prueba en un proceso judicial y de qué manera podemos ofrecer y producir dichas probanzas.

Palabras clave: *criptoactivos, nuevos sistemas, prueba.*

141 Enlace al video <https://youtu.be/KEdCMajjLgE>

142 Abogado (UNS), Diplomado en Criptoconomía: Blockchain, Criptomonedas, Smart Contracts (ITBA), Diplomado en Blockchain aplicable a los negocios y relaciones jurídicas (UCC), Director del Instituto de Derecho Informático y TICS del CABB, Mail de contacto: estudiobyb@speedy.com.ar .

INTRODUCCIÓN

En la realidad económica actual, las operaciones con criptoactivos se encuentran a la orden del día, se han masificado y adquirido una gran popularidad en nuestro país y en el mundo.

Con dicha masificación y popularidad también comienzan a aparecer los conflictos en las distintas relaciones jurídicas que se realizan con y a través de ellas.

A veces por el desconocimiento en el sistema, otras por el aprovechamiento de algunos, lo cierto es que de una u otra manera, determinados usuarios de estos “nuevos sistemas” salen perjudicados en sus derechos y en su patrimonio.

La intención del presente trabajo es analizar, de forma muy abreviada, qué elementos contaríamos para utilizar como prueba en un proceso judicial de esas situaciones y de qué manera podemos ofrecer y producir dichas probanzas.

CONCEPTOS BÁSICOS

Previo a entrar en el análisis de la prueba y de cómo probar, es necesario desarrollar muy abreviadamente los conceptos que estaremos utilizando.

Al hablar de criptoactivos nos referimos a un concepto más amplio del de criptomoneda ya que lo utilizamos como sinónimo de token, es decir: *“un activo digital que funciona utilizando un red P2P (peer to peer – persona a persona) como medio para el intercambio de archivos”*¹⁴³ “.

Asimismo, dentro de estos conceptos podemos definir a las criptomonedas como *“monedas virtuales de emisión descentralizada sin respaldo de ningún gobierno o entidad en particular basadas en tecnología blockchain.”*¹⁴⁴

A su vez, la tecnología blockchain, de manera resumida la podemos definir como una base de datos descentralizada y distribuída entre distintos nodos, accesible a todo público, con capacidad de verificación descentralizada y completamente segura por su sistema criptográfico.

La tecnología blockchain hace alusión a una cadena de bloques en la cual cada bloque contiene la información de todas las transferencias de criptoactivos, asimismo estos bloques están distribuidos en varios nodos (computadoras), y

¹⁴³ “Las criptomonedas y su naturaleza jurídica en el derecho comparado y Argentina” Denoya Rolla, Pablo Daniel – Escuela de Económicas y Jurídicas – Universidad Nacional del Noroeste Bonaerens

¹⁴⁴ Extraído de “Primer caso argentino de apropiación de criptomonedas” – Andres Chomczyk; Pablo Palazzi – Diario la Ley – AR/DOC/833/2019

permite el acceso público, es decir cualquier persona puede verificarlo.¹⁴⁵

Es importante aclarar que existe una clasificación de sistemas de blockchain entre públicas y privadas o permissionadas, teniendo como principal diferencia que, mientras en las primeras la información estará disponible para cualquier persona; en las blockchain permissionadas, solamente aquellos usuarios a los que se les entreguen las claves pertinentes podrán hacer uso de las mismas.

Por otro lado, toda la información que allí se cargue tendrá un carácter de inmutable, es decir no podrá ser borrado ni modificado por ninguna persona.

ACTIVIDAD PROBATORIA

Teniendo los conocimientos básicos de los conceptos que están en juego, procederemos a analizar cómo llevar adelante la actividad probatorio en conflictos donde estén en juego criptoactivos.

En este punto debemos analizar que los posibles problemas que vemos están relacionados con obligaciones donde los criptoactivos son utilizados o bien como

¹⁴⁵ Para mayor información acerca del funcionamiento del sistema Blockchain recurrir a “Las Nuevas Tecnologías y el Derecho” – Fernando Branciforte – Diario La Ley 22/7/2019 – AR/DOC/2232/2019

forma de pago o como forma de intercambio.

Aquí vale hacer alusión que los criptoactivos son aceptados legalmente en nuestro derecho e incluso tienen gran cantidad de regulación considerándose por la mayoría de la doctrina con una naturaleza de cosa virtual.

Así las cosas, como primer medida, aquella parte que quiera comprobar que cumplió su obligación de transferir los criptoactivos en cuestión, deberá recurrir a la blockchain base en la cual la operación se llevó a cabo.

Recordemos que, al día de la fecha, existen gran cantidad de sistemas blockchain siendo las dos más conocidas Bitcoin y Ethereum, pero también existen Blockchain de tipo permissionadas o privadas que utilizan otros servicios como es el caso de Hyperledger de IBM/Linux.

Con lo cual, a la hora de ofrecer la prueba, como primer punto a analizar debemos ver si la operación de transacción se realizó en una blockchain pública o en una permissionada.

TRANSACCIÓN REALIZADA EN BLOCKCHAIN PÚBLICA

Si la transacción fue realizada en una Blockchain de tipo pública, para

comprobar que la transacción se efectivizó nos bastará con acceder a la web en la cual se encuentran todas las transacciones y buscar la nuestra¹⁴⁶.

Aquí es importante aclarar que en los exploradores blockchain lo que nosotros veremos será el código hash del bloque, deberemos acceder al hash para ahí encontrar nuestra transacción que estará individualizada conforme las direcciones de envío y recepción. El hash del bloque que se creó nos aparecerá como un registro (simil comprobante) cuando nosotros realizamos la transacción.¹⁴⁷

Con lo cual, en cualquier computadora se podrá ver que transacciones se realizaron, por cuanto monto, en que horario, en que hash de bloque quedó registrado y toda la información que nosotros teníamos.

En este sentido, debiéramos acompañar como documental, capturas de pantalla de la página web en la cual se observa toda la información nombrada, en conjunto con la información de nuestra dirección pública que surge de nuestra wallet privada.

¹⁴⁶ Para ello deberá ingresar a la web www.blockchain.info seleccionar explorador y ahí buscar el explorador de la Blockchain sobre la que realicé la operación para poder ver todas las transacciones que allí se encuentran.

¹⁴⁷ Es importante aclarar que esto dependerá si la transacción se realizó por medio de P2P o utilizando algún intermediario como un Exchange, pero tal análisis no lo realizamos por la brevedad del presente trabajo.

Por otro lado, a efectos de generar una mayor fuerza probatoria, es recomendable que dichas capturas se hagan en presencia de un escribano público a efectos de que forme un acta con todo el procedimiento a realizar en la investigación.

Asimismo, recomendamos que se solicite como prueba pericial informática la designación de un perito que, teniendo a la vista nuestra wallet, ingrese a la web www.blockchain.info y analice si la transacción se llevó a cabo, de que dirección a cual, en qué momento, con qué número de hash, etc.

Entendemos que con ello debiera quedar demostrado que la transacción se efectivizó o no.

TRANSACCIÓN REALIZADA EN BLOCKCHAIN PRIVADA

En este tipo de blockchain, como dijimos la información no es pública con lo cual entendemos que debiera solicitarse el libramiento de oficio a la entidad que administre la blockchain a efectos de que brinde toda la información respecto a si de nuestra dirección pública de wallet se efectivizó alguna transacción, a cual dirección se dirigió, en que bloque, el hash del bloque, etc.

CONCLUSIÓN

Como conclusión podemos analizar que la masificación actual en la utilización de los criptoactivos lleva a que cada vez aparezcan más y más conflictos, que van desde incumplimientos en obligaciones porque se desconoce la efectivización de la transacción, hasta conflictos con los propios Exchanges¹⁴⁸ donde luego de adquirir o recibir determinada cantidad de criptoactivos los mismos no se reflejan en la wallet.

Sin embargo, todas estas operaciones son fácilmente verificables y conforme el principio de amplitud probatoria nos permite recurrir a los mismos sistemas blockchain para verificar las operaciones en pugna.

¹⁴⁸ Casas de cambio que se suelen utilizar para la adquisición de criptoactivos

IMPACTOS PENALES Y CIVILES DEL RANSOMWARE¹⁴⁹

María José Quintana Dourado¹⁵⁰

RESUMEN

Los ataques de Ransomware han tomado trascendencia pública afectando a importantes instituciones públicas y privadas en Argentina y el mundo. Este fenómeno complejo y pluriofensivo, es un desafío para el derecho procesal, por cuanto la prueba de su existencia resulta difícil de producir y requiere la intervención de peritos forenses especializados.

A lo largo de este trabajo se analizará en primer lugar el encuadre del Ransomware dentro de los tipos penales vigentes en el Código Penal Argentino viendo qué bienes jurídicos se ven afectados; en tanto en segundo lugar se ponderarán las consecuencias que un ataque de Ransomware puede acarrear a su víctima, y si ésta puede verse en la obligación de responder frente a terceros.

Finalmente a modo de conclusión se traerá las buenas prácticas para protegerse de un ataque y cuáles son las claves a tener en cuenta en la investigación de un caso.

Palabras clave: Inteligencia artificial. Proceso penal. Prueba. Verdad. Motivación.

149 Enlace al video <https://youtu.be/71OXFrEEcII>

150 Abogada Especializada en Derecho Ambiental, Colegio Público de Abogados de Comodoro Rivadavia. Notaria. Investigadora en Ciber Derecho. Mail: majosequintana@gmail.com

INTRODUCCIÓN

Mediante la siguiente presentación analizaré el fenómeno del ransomware como delito: a quienes afecta directa e indirectamente; detectando cuáles son las consecuencias que puede implicar desde la responsabilidad civil en cuanto a protección de datos se refiere. Posteriormente ponderaré los desafíos procesales que implica su investigación en el proceso penal. Para finalizar, a modo de conclusión enumeraré ciertas prácticas recomendables para prevenir este tipo de ataques.

QUÉ ES, Y A QUIÉNES AFECTA UN ATAQUE DE RANSOMWARE

El ransomware es un tipo de software malicioso diseñado para mantener captivo un sistema de computación o los datos que contiene. Trabaja generalmente encriptando los datos de la computadora con una clave desconocida para el usuario. Si bien es común que sea introducido a los sistemas aprovechando alguna vulnerabilidad (puertas traseras), hoy en día, con el aumento del teletrabajo y el uso masivo de la red, suele penetrar mediante engaño a las personas a través de ingeniería social, por correos con

phishing o re direccionando a páginas web apócrifas infectadas con malware.

El ransomware afecta a cualquier usuario, negocio o actividad que pueda pagar a cambio de la devolución de su información: usuarios domésticos, negocios, gobiernos e incluso servicios críticos como hospitales o centrales energéticas, causando pérdidas temporales o permanentes de información, interrumpiendo la actividad normal, ocasionando pérdidas económicas para restaurar los sistemas y ficheros, y en algunos casos daños de reputación. En Argentina y el mundo han surgido desde la pandemia por la COVID19 algunos casos resonantes, que incluyeron la muerte de un paciente en Alemania¹⁵¹. Y lo peor es que la gran mayoría de este tipo de incidentes integra la *cifra negra* del delito, ya que no son denunciados.

Teletrabajar, hoy se volvió algo común, y a diario se abren correos institucionales desde servidores poco seguros, o se accede a los sistemas de una organización sin tomar las medidas de seguridad adecuada (como el uso de

151 <https://www.xataka.com/seguridad/ataque-ransomware-a-hospital-alemania-pudo-ser-causante-muerte-paciente> ; <https://www.elpatagonico.com/el-ciberataque-altamira-no-tiene-precedentes-n5134808>

VPN). Esto por la falsa sensación de seguridad que genera en el hombre promedio el estar en casa. Que como contra cara de la moneda, se convirtió en una “oportunidad” para los ciber delincuentes.

Estos ataques pueden estar dirigidos desde otros países, y con mucha antelación, penetrando en un sistema para luego activarse a una fecha determinada mucho tiempo después, con lo que resulta complejo rastrearlos.

Tenemos dos categorías de afectados: el que sufre el ataque y luego la extorsión, que solicita un pago a cambio de dar las llaves para des encriptar los sistemas; y por el otro eventualmente, los titulares de esa información sensible.¹⁵² Como hablamos de bases de datos afectadas, podemos incluir a un número mucho mayor de damnificados. Pensemos por ejemplo en el caso de una institución de salud que no puede acceder a las historias clínicas de sus pacientes. Quien haya realizado ese ataque se está haciendo de un valioso stock de información que luego puede vender en el mercado negro de Internet (dark web).

QUÉ DELITOS ENCIERRA EL RANSOMWARE?

Cuando hablamos de un ataque por ransomware tengamos presente que se afecta el derecho de propiedad, a través del daño a los sistemas y mediante la extorsión que exige el pago de un rescate. En primer lugar tendremos la introducción de un programa destinado a causar daños dentro de un sistema informático, esto es el malware en sí, que infecta el sistema y encripta información. Esta es la acción típica del tipo penal del delito de “daño informático” que fuera incorporada como 2do párrafo al art. 183 del Código Penal, mediante la Ley 26.388, del año 2008. Este delito sin embargo no exige para su configuración la existencia de un resultado dañoso. *“El hecho que exista un sistema de back up, como sucede en la mayoría de las empresas en modo alguno altera el delito de daño, pues la restauración requiere un esfuerzo que ya implica reparar el daño causado. Por ello se afirma que no se requiere para su configuración de un daño sino que por el contrario, representa un delito de peligro y no de resultado.”*¹⁵³ Constituyendo un delito de peligro.

¹⁵² Ley de Protección de Datos Personales, N° 25.326, Art. 2

¹⁵³ <http://www.rubenfigari.com.ar/dano-informatico-arts-183-2%C2%BA-parr-y-184-incs-5%C2%BA-y-6%C2%BA-del-c-p-ley-26-388/>

Dado que esta intromisión se comete con el propósito de obtener un beneficio económico, configura una extorsión, “*el que con intimidación obligue a otro a entregar o depositar dinero*”. Aquí la intimidación se da por la falta de acceso a datos y sistemas que puede perpetrarse *ad eternum* si no se paga el rescate.

Dicho rescate, se pide sea pagado mediante transferencia de una determinada cantidad de criptomoneda a una billetera virtual, para evitar el rastreo y garantizar el anonimato de su destinatario.

Si hasta este punto tenemos el concurso de al menos dos delitos, hay que tener presente también la naturaleza de los datos y la sensibilidad que algunos de estos pueden implicar, con lo cual se están violando secretos, de parte de quien instaló ese ransomware quien ahora accede a una gran cantidad de información. Por ello, también puede encuadrar este tipo de hecho en el delito de violación de secretos¹⁵⁴

RESPONSABILIDAD DE LAS VÍCTIMAS FRENTE A TERCEROS

Las instituciones que son blanco de ransomware pueden ser responsables civilmente frente a los titulares de esos datos que tratan, ya que son responsables por su protección. Al filtrarse esos datos, pueden eventualmente hacerse públicos y traer perjuicios para sus titulares. Por ende la Ley de Protección de Datos impone un especial deber de cuidado al *responsable o usuario del archivo de datos quien debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales*. Prohibiendo registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Por ello, quien sufre un ataque de este tipo, para eximirse de responsabilidad aquiliana frente a los titulares de los datos, deberá demostrar que la intromisión fue de una naturaleza tal que no pudo ser previsto por el estado de arte actual, o que siendo previsto no pudo evitarse (caso fortuito). Por cuanto, el régimen de la responsabilidad civil previsto en el Código Civil y Comercial, su

154 Art. 153 bis Código Penal.

especial deber de cuidado le impone un esfuerzo mayor que al promedio.¹⁵⁵

UN DESAFÍO PARA TODOS LOS ACTORES SOCIALES

Ante un delito tan complejo como este, debe tenerse presente que es fundamental la preservación de la evidencia digital, tanto para poder desinfectar los sistemas y descryptar los archivos cifrados. Pero también para garantizar que la investigación garantice el derecho constitucional de debido proceso. Por lo cual la denuncia ante policía o fiscalía especializada en ciberdelitos, permite que al investigarse el hecho se forme una base de datos con el tipo de ransomware utilizado y se podrá cotejar con aquellos que han atacado en otros lugares, y eventualmente habrá mayores posibilidades de dar con las llaves.

Existen registros públicos que contienen claves de ransomware que ya han sido descubiertos, que son de acceso público, el más conocido es www.nomoreransomware.org

Es fundamental que el atacado nunca pague el rescate, porque trata con delinquentes y no hay garantía alguna de

¹⁵⁵ Código Civil y Comercial de la Nación, Arts. 1710 y 1730.

que cumplan su promesa. También porque pagar lo pone en una situación de mayor vulnerabilidad y puede ser víctima de futuros ataques.

Si existiesen terceros cuyos datos se hayan afectado por el ataque deberán ser notificados junto con la autoridad de aplicación en materia de protección de datos. En países como España, es una práctica obligatoria por el RGPD.

La evidencia en estos casos es digital al 100% e implica personal altamente capacitado y con las herramientas de software necesarias para la investigación; lo cual es costoso. El Estado debe apuntar en su política de seguridad, a fortalecer a estos cuerpos de investigación, brindando las herramientas y capacitación necesarias ya que hoy por hoy más dependen de los esfuerzos personales de quienes se dedican a esto. Los particulares deben invertir en capacitar a su personal, tanto como lo hacen en firewalls o antivirus.-

BIBLIOGRAFÍA

- Figari, Rubén E. "Daño informático (arts. 183, 2º párr. y 184 incs. 5º y 6º del C.P. Ley 26.388)" Disponible en <http://www.rubenfigari.com.ar/dano-informatico-arts-183-2%C2%BA-parr-y->

[184-incs-5%C2%BA-y-6%C2%BA-del-c-p-ley-26-388/](#)

- Pastor, Javier. Nota periodística “Un ataque ransomware a un hospital en Alemania pudo ser el causante de la muerte de una paciente”. Disponible en <https://www.xataka.com/seguridad/ataque-ransomware-a-hospital-alemania-pudo-ser-causante-muerte-paciente>

- Nota periodística Portal “El Patagónico” El ciberataque a Altamira no tiene precedentes” 20/09/2020. Disponible en <https://www.elpatagonico.com/el-ciberataque-altamira-no-tiene-precedentes-n5134808>

TERCERA PARTE: Enseñanza e investigación en Derecho y Nuevas Tecnologías

por Corina Andrea Iuale

La tercera parte del Encuentro, en la que se recibieron y agruparon comunicaciones vinculadas con la enseñanza del derecho y las nuevas tecnologías nos puso frente a una nueva problemática cuál es la de hacer pie frente al reto de la tecnología en su relación con el derecho pero no solo viviendo esta relación en sí, sino además atendiendo a la forma de transferencia de la misma. Así se

han presentado trabajos incluso fundamentando la necesidad de la creación de cátedras que comprendan los mencionados contenidos.

En materia de investigación, se han presentado trabajos atinentes a problemas no resueltos así como también a problemas que han sido abordados por la jurisprudencia recientemente.



Capítulo 5



INTERACCIÓN DEL DERECHO Y LAS TECNOLOGÍAS: RETO PARA UNA NUEVA SOCIEDAD CON CONCIENTIZACIÓN DIGITAL¹⁵⁶

Edda Karen Céspedes Babilón^{157*}

RESUMEN

La carrera de Derecho en la Universidad Nacional de Río Negro incorporó en su Plan de Estudios Obligatorio la asignatura Derecho Informático, ubicándola así como una de las primeras carreras de universidades públicas del país en tener esta política de formación. Ello entendiendo que resulta necesario que los futuros profesionales del Derecho en todas sus funciones conozcan la relación entre su actividad y las nuevas tecnologías. Por lo que se busca estimular la lectura, el estudio y el análisis crítico en los temas que hacen a la relación entre el derecho y las tecnologías de la información y las comunicaciones.

El Derecho Informático representa un área de vacancia en la formación jurídica con impacto en el ejercicio profesional del Derecho, el acceso a la justicia y el estado de derecho en la sociedad de la información.

Ello ha impulsado a desarrollar actividades de investigación y extensión en múltiples temas vinculados con el derecho aplicado al ciberespacio.

156 Enlace al video <https://youtu.be/M1Q0He3VHMY>

157* Abogada Investigadora y Fedataria Juramentada especialista en Derecho Informático y TIC. Directora y Fundadora de Interactuemos Derecho Tecnología y Ciencia – IDTC. Miembro del Consejo Consultivo Nacional de Informática de la Presidencia del Consejo de Ministros PCM-SEGDI – mail: kcespedes@infonegocio.net.pe - <https://www.facebook.com/EddaKarenCespedesBabilon/> - www.linkedin.com/in/eddakarencespedesbabilon

PALABRAS CLAVE: Derecho Informático, enseñanza, innovación, formación profesional - ciberderechos

INTRODUCCIÓN

Vivimos un vertiginoso crecimiento en la Tecnología, cuya necesidad de uso ha sido extremadamente impulsada por los tiempos actuales de crisis, causando significativos cambios en nuestra vida familiar, laboral y profesional; y en consecuencia, se fue manifestando en la ciudadanía, cierta confusión por el obligatorio aislamiento social, que conllevó a la sociedad en general, a desenvolverse rápidamente en un ambiente digital dentro de una mezcla de desconcierto y temor, principalmente por el desconocimiento a lo que nos enfrentábamos, y la extrema necesidad de conocer y manejar las herramientas digitales, sin darnos tiempo de tomar conciencia adecuada del impacto de la Transformación Digital, impulsada apresuradamente por ésta crisis.

En ese sentido, fue menester desenvolvernos desde nuestros hogares, en actividades necesarias como Educación y Trabajo, originando, en muchos casos, un desorden y stress social que, en la actualidad, aún necesita de muchos esfuerzos para restablecer el

orden y la tranquilidad que permitan dar paso al conocimiento y uso adecuado de las Tecnologías.

Dentro de éstos avatares, el Derecho como ciencia y disciplina de regulación y normatividad, juega un rol importante en nuestra sociedad, que responsabiliza a todos los profesionales a trabajar arduamente; no sólo para evitar que el Derecho quede rezagado en el tiempo soslayando la modernidad de la Tecnología y la Ciencia, sino, además, nos convoca a realizar un trabajo investigativo que permita resaltar al Derecho como baluarte de valores, justicia y respeto por los Derechos fundamentales de la Persona inserto en los Derechos Humanos, que deben prevalecer en temas tan importantes como la evolución de los algoritmos, la neurociencia, la robótica, el Internet de las Cosas y en general todo lo referente a la Inteligencia Artificial que se torna en un ente principal de controversia y estudio, ahondándose la prioridad y respeto del marco constitucional y la Protección de los Datos Personales; asimismo, resguardar y actualizar el marco legal de

los Delitos Informáticos, como el Cibercrimen, la Ciberseguridad, la Seguridad de la Información, además de la evolución del Teletrabajo, Telemedicina, Telesalud, Teleeducación y otros rubros de avances tecnológicos y nuevos descubrimientos científicos cuya necesidad de investigación y aplicación de un marco regulatorio se tornan prioritarios.

Ésta situación de necesidad normativa y regulatoria, obliga a los Gobiernos y Estados a tomar cartas en el asunto, siendo menester priorizar la convocatoria a profesionales calificados y multidisciplinarios, con el fin de interactuar en un equipo de trabajo exclusivo para la “Concientización Digital” de toda la ciudadanía, donde emerja la adecuación a una verdadera Transformación Digital basada y enraizada en una labor sostenible de Alfabetización y Educación que llegue a todas las zonas del país, con el fin de generar una “Cultura Digital”, que nos permita como Estado y Sociedad afrontar los nuevos retos del impacto tecnológico y científico.

PROBLEMA

El desconocimiento de la ciudadanía, en general, sobre el impacto del avance de las tecnologías, y la falta de interacción de disciplinas tan importantes como el Derecho, han originado un atraso socio-tecnológico que se ve afectado actualmente en la economía de muchos países.

OBJETIVO

Conocer la importancia de la interacción del Derecho con el avance de las Nuevas Tecnologías y la Ciencia, creando un marco legal que permita su progreso basado en los valores humanos, los derechos fundamentales de la persona y en el acceso a la Educación y Concientización Digital desde la ciudad hasta las zonas más alejadas del país.

MARCO TEÓRICO

Durante algún tiempo atrás, en Latinoamérica, el tema de la Transformación Digital venía dando sus pasos en diversos países, quizás en algunos más que en otros, pero lo certero y sin duda alguna, es que la crisis

pandémica no sólo aceleró su proceso, sino que, además, nos obligó intempestivamente a afrontar una nueva realidad sin estar completamente preparados.

Éste nuevo mundo transformado por las tecnologías y la ciencia debe iniciarse con la base de ciertos conceptos indispensables e imprescindibles para el manejo adecuado de las herramientas digitales y asimismo prepararnos en un marco de concientización digital, que nos permita evitar los peligros y riesgos por el mal uso que, los ciberdelincuentes y las personas sin escrúpulos, les dan a las nuevas tecnologías.

INTERNET

El mundo se revolucionó, desde que nació Internet, (*International Network of Computers*), allá por los años 60, llamada también la “Red de Redes”, o descrita en sus orígenes como la “Red Galáctica”¹ (*Galactic Network*) por J.C.R. Licklider² del MIT³, cuyo concepto es muy similar al Internet de hoy. Una versión muy conocida es que Internet nació como ARPANET, en respuesta al Departamento de Defensa de los Estados Unidos de Norteamérica, en la Guerra Fría; sin embargo, fue Licklider como director del Programa de Investigación informática de

DARPA, (1962) quien, seguido por Ivan Sutherland, Robert Taylor y Lawrence G. Roberts, desarrollan el proyecto, que continua en investigación y avance por Leonard Kleinrock, Paul Baran y otros más.

Lo cierto es que Internet revolucionó la Informática y las comunicaciones interconectando a las personas con diferentes computadoras a nivel mundial y actualmente el número de usuarios de Internet se viene incrementando exponencialmente debido al uso de los dispositivos móviles.

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES - TIC

Internet es una fuente de información y conocimiento y sus servicios múltiples van en crecimiento, como el uso de la Web⁴, correos electrónicos, telefonía, transmisión de datos multimedia, mensajería instantánea, redes sociales, videojuegos, plataformas de intercambio de archivos, plataformas multimedia (audio y video), comercio electrónico y muchos otros desarrollos de las Tecnologías de la Información y las Comunicaciones (TIC), a las cuales podemos acceder mediante Internet, que en sí misma es parte de las TIC.

Por lo expuesto las TIC son el conjunto de tecnologías que permiten el acceso, producción, transmisión, procesamiento, almacenamiento, recuperación y tratamiento de la información y que se desarrollan a partir de los avances científicos producidos en los ámbitos e interacción de la informática y las telecomunicaciones.

CIBERDELITOS

Los Ciberdelitos son aquellas actividades ilícitas o antijurídicas cuyo fin malsano es causar daño, provocar pérdidas o impedir el uso de los sistemas y redes informáticas

Los ciberdelitos afectan a un conjunto de bienes, que pueden ser dirigidos hacia las personas, a las empresas o a los intereses colectivos, y tienen diferentes modalidades como:

- **Ciberacoso:** Violan los derechos fundamentales de la persona, como el derecho a la privacidad e intimidad, derecho al honor y la dignidad de la persona, estos delitos generalmente se suscitan a través de las Redes Sociales con calumnias y amenazas y/o el chantaje sexual llamado Sextorsión⁵.
- **Grooming:** Una indignante figura delictiva, que tiene diferentes

modalidades, como aquellos realizados por ciberdelincuentes pedófilos quienes atentan sexualmente contra los menores de edad.

- **Phishing:** Otra modalidad de ciberdelito que hace uso de la ingeniería social o técnicas de engaños utilizada por ciberdelincuentes, valiéndose de la buena fe del usuario final, para lograr obtener y robar información sensible bajo la fachada de un sitio confiable (https)⁶, mediante este método logran obtener claves de acceso, números de tarjetas bancarias y toda información sensible⁷ de la víctima, producto de este engaño; logrando la suplantación de identidad o la clonación de tarjetas.

- **Ciberdelitos de alta tecnología:** Es necesario resaltar los delitos de alta tecnología, originados por Malwares⁸ y Ransomware⁹ que afectan principalmente al sector financiero mundial, en esa categoría podemos mencionar serios delitos de extorsión, operaciones fraudulentas por Internet, sabotaje informático, tráfico ilegal de datos personales, y en general toda operación financiera y comercial engañosa, causada por el acceso no autorizado a los sistemas informáticos, conocido como piratería informática (cracking)

Para evitar los ciberdelitos es necesario tener una política de Ciberseguridad.

CIBERSEGURIDAD

La ciberseguridad es el marco global del cuidado monitoreo y protección tanto de datos como de plataformas informáticas en el cual se aplican políticas de seguridad informática para evitar acciones delictivas sobre estos activos. (Leonett, J. R.)

INTELIGENCIA ARTIFICIAL

Fue en el año de 1956 que John McCarthy¹⁰ lanza el concepto de Inteligencia Artificial definiéndola como la ciencia e ingeniería de hacer máquinas inteligentes.

La comunicación de la Comisión Europea¹¹ en el Plan coordinado sobre Inteligencia Artificial, indica: "...se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos..."

Con éstos y otros antecedentes teóricos y prácticos se puede definir que la

Inteligencia Artificial (IA) es una tecnología digital que combina algoritmos en un programa, con el fin de crear máquinas que proporcionen capacidades como interpretación, decisión y resolución de problemas.

El sofisticado avance de la IA genera controversias en su comparación con el ser humano, sin embargo, es indudable el crecimiento acelerado de proyectos innovadores en sectores estratégicos, que traen consigo un impacto en el desarrollo de la economía a nivel mundial (Céspedes B., E.K. IDTC)¹²

La IA trabaja a través de algoritmos y está muy ligada al Internet de las Cosas y la Robótica

- **Algoritmo** es un conjunto de instrucciones y pasos lógicos necesarios, o reglas definidas, finitas y jerarquizadas, que permiten llevar a cabo una tarea específica, solucionar un problema o situación planteada, procesar datos, analizar, efectuar toma de decisiones y realizar otras tareas o actividades. Por ejemplo: Google cuenta con un algoritmo para su sistema de búsqueda y posición de páginas. Otro ejemplo es el contenido de las Redes Sociales que está regido por algoritmos que permiten la interacción con los usuarios. (Céspedes B., E.K. IDTC)¹³

- Internet de las Cosas

También llamado “IoT” (*Internet of Things*), el creador del “Concepto el Internet de las Cosas” es Kevin Ashton. IoT se refiere a la interconexión digital con Internet, de objetos físicos que por intermedio de circuitos integrados, sensores y conectividad, permiten el intercambio automático de información y datos con otros dispositivos inteligentes y centros de control.

Inicialmente la IoT surgió para interconectar objetos domésticos; pero actualmente se vienen realizando aplicaciones en la vía pública, las instituciones y al interior de las empresas. (Céspedes B., E.K. IDTC)¹⁴

- Robótica

La Robótica es la creación de Robots. Se ocupa del diseño, construcción, operación, estructura, manufactura, y aplicación de los robots que le permita realizar diversas tareas en diferentes áreas, combinando múltiples disciplinas como la mecánica, la electrónica, la Informática, la Inteligencia Artificial, la Ingeniería de Control y la Física.

Es importante mencionar que, dentro de estos conceptos mencionados, con fines académicos, el rol de los Datos

Personales constituye una materia importante en el buen uso de las herramientas digitales y dentro del respeto de los derechos fundamentales de la persona. Es decir, la regulación de la Protección de Datos Personales debe figurar con notable relevancia, dentro del marco jurídico de cada país en paralelo al continuo avance tecnológico actual.

RELEVANCIA DE LA INTERACCIÓN DEL DERECHO Y EL AVANCE TECNOLÓGICO EN EL SIGLO XXI

Una de las formas tradicionales e iniciales de concebir la interacción entre el Derecho y las Tecnologías es a través del contexto de la Informática Jurídica que considera la aplicación de la informática como un instrumento para el Derecho, constituyéndose en un objeto de estudio y reglamentación; de ahí se origina la necesidad de una rama del Derecho que se encargue de regular los efectos y controversias jurídicas originadas por el uso masivo de los sistemas informáticos.

DERECHO INFORMÁTICO

El Derecho Informático, nace como una rama del derecho especializada en el tema de la informática; sus usos, aplicaciones e implicaciones legales, las cuales ameritan el surgimiento de nuevas

normas jurídicas y/o la actualización de las existentes.

El Derecho Informático abarca muchas otras ramas del Derecho partiendo de los principios constitucionales, que protegen los derechos fundamentales de la persona como la intimidad, el honor, la dignidad y el uso ilegal de los sistemas informáticos; que son violados mediante correos electrónicos, mensajerías instantáneas o las redes sociales que se han masificado; en ese sentido el rol del Derecho Penal se hace necesario para salvaguardar la violación de éstos y otros derechos. En el caso del Derecho Civil, tomaré el ejemplo de la regularización de las notificaciones electrónicas que ameritan un gran avance en los procesos judiciales, así como la regulación de la Manifestación de Voluntad por medios electrónicos, (artículo 141-A del Código Civil Peruano), y la firma Digital, en el Perú con la Ley 27269 Ley de Firmas y Certificados Digitales (26may2000); normas que han facilitado el desarrollo del Comercio Electrónico. Cabe resaltar que el Perú es el único país que desde el año 1991, a través del Decreto Legislativo 681 (14oct1991), crea la figura del Fedatario Juramentado con especialidad en Derecho Informático, quien, como dador de Fe Pública, utiliza la Firma y el

Certificado Digital como herramientas necesarias para garantizar la Seguridad Informática y la Seguridad Jurídica.¹⁵ (Céspedes Babilón, E.K)

LA IMPORTANCIA ACTUAL DEL TELETRABAJO

El Teletrabajo es legislado en muchos países pero carente de una previa y adecuada capacitación ha traído innumerables contradicciones al respecto del intempestivo confinamiento domiciliario y obligación de las personas a trabajar desde casa, en ese sentido el Perú cuenta con la Ley 30036 Ley del Teletrabajo (05jun2013) que cubre derechos y obligaciones laborales e indica la voluntariedad del trabajador para tomar ésta alternativa laboral; pero para evitar la propagación del Coronavirus, se publicó el Decreto de Urgencia 026-2020 donde se establecen diversas medidas excepcionales entre las cuales se configura el Trabajo Remoto (art. 16 y 23) el cual establece el deber de realizarlo desde el domicilio del trabajador subordinado, mediante herramientas tecnológicas, según sea el caso. La figura del Trabajo Remoto, trajo consigo innumerables controversias y problemas sociales, que aún siguen en vigencia, debido a la obligatoriedad, el

desconocimiento del trabajador en el uso de las herramientas digitales, la falta de infraestructura del trabajador, el abuso del empleador fuera de las horas laborales, el recargo de las tareas domésticas y familiares, y en general la falta de prevención de seguridad informática o ciberseguridad, que trae consigo la exposición de la privacidad, la protección de datos personales y en general la exposición al trabajador y la empresa extendiéndose a los miembros de las familia debido a la intromisión ilegal de la ciberdelincuencia.

EL CRECIMIENTO DE LOS CIBERDELITOS

En el uso de la Tecnologías es importante destacar la penosa masificación de la intrusión de los Ciberdelincuentes, con actitudes sociópatas,¹⁶ quienes a través de diferentes técnicas y recursos comenten acciones criminales o al margen de la Ley causando graves daños.

Con respecto a los **Ciberdelitos** es importante mencionar al tratado internacional denominado “Convenio contra la Cibercriminalidad”, mejor conocido como el “Convenio de Budapest” cuyo objetivo es la lucha contra la ciberdelincuencia basada en la aplicación

de un marco jurídico y política penal en armonía mundial. El Perú cuenta con la Ley 30096, Ley de Delitos Informáticos y es uno de los países adheridos a este Convenio internacional, por lo que debemos seguir sus lineamientos, y asimismo mejorar y/o adecuar nuestras normativas y políticas públicas para seguir avanzando en el combate contra el cibercrimen, debido a que somos el quinto país de Latinoamérica que recibe mayor cantidad de ataques cibernéticos. Según la División de Investigación de Delitos de Alta Tecnología (DIVINDAT)¹⁷, los ataques que recibe nuestro país son de fraudes electrónicos, abuso sexual infantil, suplantación de identidad. y ataques que en su mayoría afectan al sector financiero.

LA REDES SOCIALES, LA PRIVACIDAD Y VIOLENCIA DIGITAL

La privacidad como factor importante de respeto y derecho de las personas se hace vulnerable por el desconocimiento de la adecuada protección de los contenidos que se publican en los diferentes medios digitales. En este sentido, las Redes Sociales, no sólo se utilizan en el marco de la comunicación, diversión amistad y conocimiento, que fue el inicio de su creación; sino que se han convertido en un foco de Violencia

Digital¹⁸. Estos contenidos voluntarios e indiscriminados son realizados, en general, por los mismos cibernautas, haciendo pública su vida, su familia, amigos, lugares visitados, conexiones, etc., ocasionando una excesiva información que puede ser utilizada y configurada en perfiles sistematizados (Big Data)¹⁹ para el marketing de algunas empresas con el fin de generar aumento en sus ventas; pero también son utilizados por los ciberdelincuentes para sus propios fines delictivos. Los individuos que realizan Violencia Digital se constituyen en el prototipo de persona de bajos instintos, con personalidad agresiva y fines de hacer daño. (Céspedes Babilón, E.K.)

LA DISRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL (IA)

En el caso del sofisticado avance de la Inteligencia artificial, es necesario resaltar que la IA actualmente ayuda a resolver problemas de salud y seguridad y ha sido de gran impacto en la lucha contra la pandemia. Asimismo, ha generado gran avance en la Agricultura con drones y sistemas inteligentes y otros campos y profesiones como el Derecho donde la eficacia y rapidez se constituyen en una mejor atención en los procesos y

resoluciones judiciales. Sin embargo, la IA ha generado muchas controversias con el respecto a la violación de los derechos fundamentales de la persona y los valores humanos como la Moral y la Ética, por otro lado, existe cierto temor de que la IA reemplazará al ser humano. Estas premisas y dudas se fundamentan en que la IA puede ser discriminatoria, y sesgada, como se ha visto en el caso del algoritmo de los vehículos autónomos²⁰ y las resoluciones judiciales del algoritmo “Compass”²¹ en EEUU. Estas controversias sobre su uso y los valores humanos como la Ética se generan en muchos campos y son materia de discusión y necesaria regulación.

Aún no tenemos una normatividad jurídica al respecto de la Inteligencia Artificial; pero existen algunos organismos internacionales que vienen ocupándose de su regulación y la “Ética” que debe primar en su uso. Por ejemplo, en la Unión Europea se ha conformado el Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial (2019), la Comisión Europea para la eficiencia de la Justicia (CEPEJ) que emite la Carta Ética Europea (diciembre 2018) y la modernización del Convenio 108 (2018) que incluyen principios y respeto a los derechos humanos. Con ese mismo

objetivo, la UNESCO, lanzó una encuesta sobre ÉTICA, (Julio 2020) cuyos resultados están previstos para fines del 2021.

En el desarrollo de la IA y sus fines regulatorios, también es conveniente y necesario enfocarla, desde el marco de la Responsabilidad Civil, teniendo en cuenta que es el ser humano quien crea el algoritmo.

En este punto, cabe resaltar que la Inteligencia Artificial está conformada por los Algoritmos y los Datos. Por lo tanto, es importante mencionar que los Datos Personales, son un tema sensible y su utilización es primordial, no sólo en la Inteligencia Artificial, sino además en muchas materias dentro del avance tecnológico.

IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES Y LA CIBERSEGURIDAD

Actualmente, la dinámica galopante de las TIC demanda un mayor reto al Derecho Informático para garantizar el marco jurídico de protección y respeto a las leyes en aras de un orden social que garantice el desarrollo, innovación y aplicación de las nuevas tecnologías.

PROTECCIÓN DE DATOS PERSONALES

Uno de los temas más relevantes es la vulnerabilidad de la Privacidad y la Protección de Datos Personales en el uso de las tecnologías, cuando no se toman las medidas de seguridad preventivas para evitar ser víctimas del ataque de los ciberdelincuentes, de ahí la importancia de la Ciberseguridad.

Es importante mencionar al Reglamento General de Protección de Datos Personales de la Unión Europea (RGPD 2016/679) del Parlamento Europeo y del Consejo del 27 de Abril 2016 relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de Datos Personales y a la Libre Circulación de estos datos y por el que se deroga la Directiva 95/46/CE, el cual marca los lineamientos del que se rigen muchos países para la adecuación de su normativa jurídica y políticas de seguridad. El Perú ha tomado sus lineamientos y contamos con la Ley 29733 Ley de Protección de Datos Personales (03jul2011) y el Decreto Supremo 003-2013-JUS (22mar2013). Cabe mencionar que todo esfuerzo regulatorio es insuficiente, si se obvia la sensibilización de las medidas preventivas

para cumplir el objetivo de la ley; y en ese sentido, es necesaria la interacción e intervención de profesionales multidisciplinares, así como del gobierno y el Estado.

IMPORTANCIA DE LA CIBERSEGURIDAD

Las TIC fueron creadas para cubrir las necesidades y demandas de las personas, mediante herramientas que nos proporcionan enormes ventajas; pero debemos resaltar, también, que ha facilitado el ataque de ciberdelincuentes quienes utilizan estas herramientas tecnológicas para cometer sus delitos.

Las intrusiones dañinas cometidas por los ciberdelincuentes a través de diferentes modalidades pueden afectar seriamente a una persona²², una empresa, un gobierno (infraestructura crítica) o todo un país²³. Es por lo que debemos tener presente el resguardo de nuestra información y datos mediante sistemas de seguridad que nos proporcionen una navegación segura, desde nuestros hogares, centros laborales y gobierno. En ese sentido toma especial relevancia la **Ciberseguridad** como una prioridad a ser aplicada en todos los ámbitos del uso de las tecnologías, desde el ámbito personal hasta en las organizaciones, instituciones

y empresas privadas y públicas. Pero es necesario que para implantar políticas de ciberseguridad se realice una capacitación previa que involucre a todas las personas, ejecutivos y funcionarios en general creando una cultura de seguridad que parta desde la familia y los Centros Educativos para evitar intromisiones ilegales y ataques delictivos. En el caso de las empresas, la Ciberseguridad debe convertirse en una prioridad y actividad crítica para la protección de la información y cumplimiento de los objetivos empresariales, que asimismo pueden crecer con la utilización adecuada de la Inteligencia Artificial y evitar lo que indica el Ing. Leonett: *“El déficit de las medidas de seguridad y mal cumplimiento de los protocolos de ciberseguridad ha orillado al sector IT en la solicitud y socorro de la Inteligencia Artificial para corregir y mermar estos errores”*

Como vemos resulta insuficiente el marco jurídico aplicado a las nuevas tecnologías, y debemos enfrentarnos a nuevos retos, como el desarrollo vertiginoso de la Inteligencia Artificial, la Neurociencia, Computación Cuántica, el avance del Blockchain, el Bioderecho, crecimiento del Big Data, Red Cloud y otros, donde la justicia, los valores humanos y la educación deben priorizarse.

APORTES E IMPORTANCIA PRIORITARIA DE LA CONCIENTIZACIÓN DIGITAL

Para lograr una conciencia digital en la población debemos asegurarnos previamente de la Alfabetización y Educación digital que versa en la enseñanza y aprendizaje sobre el buen uso de Internet y la aplicación de las herramientas digitales. Este proceso debe incluir el marco de prevención contra las acciones lesivas a los derechos fundamentales de la persona en congruencia con la Inclusión Digital y creando una Cultura Digital, a nivel país, en favor de lograr las metas y objetivos de cada disciplina.

Por tanto, indico que “La Concientización Digital versa en el Saber Humano, que consiste en conocer, analizar, reflexionar e interiorizar el impacto del desarrollo e innovación de las ciencias tecnológicas que interactúan en nuestras vidas; asimilando a plenitud sus efectos, consecuencias e interacción en la vida de todas las personas, sea en el ambiente familiar, social, profesional, empresarial, y, en general, como ciudadanos, para lograr un cambio cultural positivo y una Transformación Digital que nos permita un

desarrollo socio económico a nivel mundial”.

En este proceso y para la objetiva reducción de la brecha digital, debe partirse por la conectividad desde la ciudad hasta las zonas más alejadas, por eso es necesario la aplicación de políticas sostenibles pero ejecutables a corto plazo donde se involucre el Estado, el Gobierno, el Sector Privado y los ciudadanos en general; porque “No podemos hablar de Transformación Digital sin Concientización Digital”

En ese sentido reitero mi convocatoria, desde aquí a ese abogado “apasionado” en su carrera profesional, que supera obstáculos y limitaciones; investigando, conociendo y compartiendo información; incentivado por ese “espíritu hacker”²⁴ que puede aplicarse a los juristas, que crean, mejoran y perfeccionan el marco legal, con el fiel objetivo de contribuir al Derecho y la Justicia. (Céspedes B., E.K.)

Asimismo, me atrevo a proponer una vez más, una Reforma Educativa que incluya cursos de valores humanos, patriotismo y desarrollos de tecnologías en el marco de la Concientización Digital, desde las aulas preescolares hasta las Universidades e Institutos Superiores.

Aún hay mucho por versar y mucho por hacer, pero nos queda asumir el reto, y difundir el respeto por la justicia, los valores y los derechos fundamentales de la persona, desde nuestra vida cotidiana y en el buen uso de las Tecnologías, para forjar, seres humanos conscientes de una cultura digital en favor de la sociedad, así como el crecimiento y desarrollo de nuestro país.

BIBLIOGRAFÍA

1. BARZANALLANA, Rafael - Biografía de Joseph Licklider “Uno de los Padres de Internet” – Departamento Informática y Sistemas – Universidad de Murcia, España

<https://www.um.es/docencia/barzana/BIOGRAFIAS/Biografia-JCR-Licklider.php>

2. CASTELLS, M. “Internet y la sociedad Red”. Lección inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento. <http://www.uoc.edu/web/esp/articulos/castells/castellsmain1.html>

3. CÉSPEDES BABILÓN, Edda Karen “Interactuemos, Derecho Tecnología y Ciencia – IDTC EKCB - Lima, Perú

<https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaIDTC>

4. CÉSPEDES BABILÓN, Edda Karen “El Fedatario Informático en el Perú” XV Congreso Iberoamericano de Derecho e Informática – FIADI 2011 Buenos Aires, Argentina

http://www.eldial.com/nuevo/congreso_iberoamericano/EL%20FEDATARIO

[%20INFORM%3%81TICO%20EN%20EL%20PER%3%9A.pdf](#)

5. CÉSPEDES BABILÓN, Edda Karen. Conferencia: “Violencia Digital y sus implicancias en el Derecho de las Personas” III Congreso Internacional de Derecho. Facultad de Derecho. Universidad San Tomás. Villavicencio, Colombia. 2017

6. CÉSPEDES BABILÓN, Edda Karen. “El Hacker del Derecho” XIX Congreso Iberoamericano de Derecho e Informática FIADI 2015 Medellín, Colombia <http://fiadi.org/wp-content/uploads/2015/08/Edda-Karen-Cespedes.pdf>

7. COMISIÓN EUROPEA – Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y social Europeo y al Comité de las Regiones – Plan coordinado sobre la Inteligencia Artificial – Bruselas 2018 <https://ec.europa.eu/transparency/regdoc/ep/1/2018/ES/COM-2018-795-F1-ES-MAIN-PART-1.PDF>

8. GUILLEN TORRES, Beatriz “El verdadero padre de la Inteligencia Artificial” <https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/el-verdadero-padre-de-la-inteligencia-artificial/>

9. INTERNET SOCIETY: “Breve historia de Internet”

<https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#:~:text=Or%C3%ADgenes%20de%20Internet,concepto%20de%20%E2%80%9CRed%20gal%C3%A1ctica%E2%80%9D.>

10. LEONETT, JOSE R. Observatorio Guatemalteco de Delitos Informáticos – OGD I – <https://ogdi.org/>

11. PRESIDENCIA DEL CONSEJO DE MINISTROS Perú se adhiere al Convenio de Budapest para luchar contra la Ciberdelincuencia

<http://www.pcm.gob.pe/2019/02/peru-se-adhiere-al-convenio-de-budapest-para-luchar-contra-la-ciberdelincuencia/>

12. UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA CSIRT Seguridad de la Información <https://csirt.utpl.edu.ec/10-consejos-para-evitar-ataques-de-phishin5>

NOTAS

1 Red Galáctica: Conjunto de ordenadores interconectados globalmente a través de los que todo el mundo rápidamente a datos y programas desde cualquier

2 Joseph Carl Robnnet Licklider uno de los padres

3 MIT: Instituto Tecnológico de Massachusetts – Universidad Privada en Cambridge, Massachusetts.

4 Web: World Wide Web o Red Informática de alcance mundial que permite interconectar sistemas de hipertexto. Para utilizar la Web se necesita un navegador como Google Chrome, Mozilla

5 Sextorsión: Chantaje sexual por la posesión de una imagen íntima.

6 https Protocolo seguro de transferencia de texto

7 ONU – Que es Información sensible?

8 Malware: Software malicioso diseñado para infiltrarse, sin autorización, en un dispositivo

9 Ransomware (secuestro de datos): Programa que impide el acceso a un sistema operativo, pidiendo un rescate a cambio de quitar la restricción.

10 John MacCarthy organiza la Conferencia de Dartmouth en 1956 donde por primera vez acuña el concepto de IA, reconocido como el Padre de la Inteligencia Artificial.

11 Comisión Europea - Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Consejo social Europeo y al Comité de las Regiones – Plan coordinado sobre la Inteligencia Artificial – Bruselas 2018

12 <https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaDTC/posts/586553578544387>

13 <https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaDTC/posts/824613844738358>

14 <https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaDTC/posts/842837086249367>

15 El Fedatario Informático en el Perú

http://www.eldial.com/nuevo/congreso_iberoamericano/EL%20FEDATARIO%20INFORM%C3%81TICO%20EN%20EL%20PER%C3%9A.pdf

16 Actuación con dolo. (José R. Leonett

17 Policía Nacional del Perú – Ministerio del Interior MININTER

18 Ciberacoso, Grooming, Cyberbullying, Phishing, Firefox, Microsoft Edge, etc.

19 Grandes volúmenes de Datos estructurados para

20 Automóviles que disponen de tecnologías

21 frenar, adelantar, estacionarse, necesidad de la conducción de una persona.

22 Algoritmo que analiza el historial delictivo y predice la reincidencia en un delito.

23 Ciberacoso, Grooming, Cyberbullying, Phishing,

24 Ciberguerras, Ciberterrorismo.

25 “El Hacker del Derecho” Céspedes Babilón, Edda Karen

FORMANDO A LOS PROFESIONALES DEL ¿FUTURO?. EXPERIENCIAS PRÁCTICAS DE FORMACIÓN¹⁵⁸

Juan M. Brussino K. y Ana E. Lambrecht^{159*}

RESUMEN

La carrera de Derecho en la Universidad Nacional de Río Negro incorporó en su Plan de Estudios Obligatorio la asignatura Derecho Informático, ubicándola así como una de las primeras carreras de universidades públicas del país en tener esta política de formación. Ello entendiéndose que resulta necesario que los futuros profesionales del Derecho en todas sus funciones conozcan la relación entre su actividad y las nuevas tecnologías. Por lo que se busca estimular la lectura, el estudio y el análisis crítico en los temas que hacen a la relación entre el derecho y las tecnologías de la información y las comunicaciones.

El Derecho Informático representa un área de vacancia en la formación jurídica con impacto en el ejercicio profesional del Derecho, el acceso a la justicia y el estado de derecho en la sociedad de la información.

Ello ha impulsado a desarrollar actividades de investigación y extensión en múltiples temas vinculados con el derecho aplicado al ciberespacio.

PALABRAS CLAVE: *Derecho Informático - Enseñanza - Innovación - Formación Profesional - Ciberderechos.*

158 Enlace al video <https://youtu.be/M4Nr7fhp3r8>

159* Profesor de Universidad Nacional de Río Negro. Juez de Garantías Poder Judicial de Río Negro.

Abogada, graduada de la UNRN. Integrante de ADIAR Contacto: aelambrecht@gmail.com

INTRODUCCIÓN

En la actualidad el uso de sistemas de información en todos los aspectos de la vida se ha vuelto ubicuo. La informatización, digitalización y conexión en redes tiene lugar en cuestiones personales, económicas, políticas, culturales y de la administración del Estado, resultando necesario que los profesionales del Derecho en todas sus funciones conozcan la relación entre su actividad y las nuevas tecnologías. En este sentido, en el presente trabajo se propone realizar un análisis exhaustivo de la experiencia en la carrera de Abogacía de la Universidad Nacional de Río Negro, como una de las primeras del país en tener dentro de su plan de estudios obligatorio, la asignatura Derecho Informático. Para ello se apuntarán cuestiones vinculadas a la lógica de estudio dentro de la asignatura y su interacción con las distintas ramas del derecho. Resulta pertinente analizar cual es el contenido obligatorio establecido en el programa analítico de la materia, al mismo tiempo que se analizan los objetivos que se persiguen con la inclusión de la misma.

La realidad actual impulsa a los profesionales a continuar con la formación básica y tradicional, pero no se puede

desconocer la absoluta necesidad de formarse en los derechos que surgen de la implementación de las nuevas tecnologías e internet en todos los vínculos de la sociedad. Cuestiones con las que abogados y abogadas cotidianamente se enfrentan en el ejercicio de la actividad profesional.

La implementación de esta asignatura, dio como resultado que simultáneamente se desarrollaran tareas de investigación y extensión en referencia a los ciberderechos. Surgiendo como consecuencia de ello equipos de investigación que han trabajado en diversos proyectos, de los cuales algunos serán apuntados en el presente trabajo.

Asimismo, la actividad de investigación llevada a cabo por los y las estudiantes ha dado como resultado numerosos Trabajos Finales de Grado en diversas temáticas que derivan del Derecho Informático.

EL DERECHO INFORMÁTICO COMO ASIGNATURA

La carrera de Derecho en la Universidad Nacional de Río Negro comenzó a dictarse en el año 2011. Desde su formación, en su Plan de Estudios se incorporó como asignatura obligatoria Derecho Informático, ubicándola como

una de las primeras carreras de universidades públicas del país en tener esta política de formación.

Desde ese entonces se entendió que el Derecho Informático representa tanto una rama establecida como un área de vacancia en la formación jurídica con impacto en el ejercicio profesional del Derecho, el acceso a la justicia y el estado de derecho en la sociedad de la información.

La realidad socio-económica-cultural en la que la implementación de las nuevas y no tan nuevas tecnologías de la información y la comunicación y particularmente el uso de internet, no se pueden desconocer en la formación que se le imparte a los y las estudiantes.

Hace no mucho tiempo se consideraba que estas temáticas tendrían implicancias en la vida futura de las personas, sin embargo, a pasos agigantados la realidad ha mostrado que ese futuro que se creía lejano, llegó hace rato.

En este contexto, con la implementación de la asignatura se busca estimular la lectura, el estudio y el análisis crítico en los temas que hacen a la relación entre el derecho y las tecnologías de la información y las comunicaciones. Tendiendo a que los futuros abogados y abogadas comprendan las cuestiones

básicas del funcionamiento y la gobernanza de Internet y propender al conocimiento por parte de los estudiantes de las diferentes fuentes del derecho aplicables a temas de privacidad, libertad de expresión, delitos y gobierno en entornos digitales. Impulsando a los y las estudiantes a la comprensión de las características del derecho informático a los fines de asesorar en materia de derechos personales, intereses patrimoniales y cuestiones públicas relacionadas al uso de las llamadas nuevas tecnologías. Sin perder de vista la necesidad de que los y las estudiantes desarrollen la capacidad de evaluar las políticas públicas con impacto en el uso y desarrollo de tecnologías de la información y las comunicaciones.

Para ello se necesita un abordaje íntegro, el cual resulta de la interacción entre las distintas ramas del derecho y las nuevas tecnologías de la información y las comunicaciones. El fenómeno telemático es estudiado en el particular efecto que tiene sobre la formación y ejecución de los contratos, la protección de los datos personales y la privacidad, la libertad de expresión y el acceso a la información, los delitos informáticos y las cuestiones procesales conexas. Se analiza la aplicación del derecho vigente, así también como las soluciones planteadas

en otras jurisdicciones y las propuestas de reforma, incluyendo las propuestas de organizaciones internacionales del ámbito estatal y privado.

Son múltiples los propósitos que se buscan con la implementación de esta asignatura, sin embargo se propende a la formación como futuros profesionales para enfrentarse a la actividad profesional tanto en el ámbito público como privado, como así también en su futura actividad en investigación y docencia.

ACTIVIDAD DE INVESTIGACIÓN

La implementación de la Asignatura de Derecho Informático ha impulsado a docentes y estudiantes a generar actividades de investigación en este área.

Ello ha dado como resultado, entre otros, el proyecto de investigación “*El Derecho Penal y la protección de menores en Internet*”, donde se analizaron las conductas nocivas para los menores de edad llevadas a cabo en entornos digitales y su captación adecuada por el derecho penal argentino. Realizando análisis comparativos, tanto de las cuestiones materiales como legales, tanto a nivel local como internacional, contemplando la punibilidad de las conductas en cuestión. Proyecto que dio

como resultado varias presentaciones en congresos y eventos académicos, resultando así también en la obtención de una Beca de Estímulo a las Vocaciones Científicas del Consejo Interuniversitario Nacional.

Asimismo se gestó el Proyecto de Voluntariado Universitario *Conectando con Responsabilidad* en el marco de la Secretaría de Políticas Universitarias del Ministerio de Educación de la Nación. Cuyo objetivo principal consistió en diseñar e implementar un proceso de información y capacitación de capacitadores y estudiantes secundarios de escuelas públicas de la ciudad de Viedma en cuestiones referentes al uso responsable y seguro de las tecnologías de las comunicaciones y de la información provistas por el Programa Conectar Igualdad con el fin de contribuir al desarrollo armónico e inclusivo de todos los sectores de la comunidad dentro de la sociedad de la información. Se buscó informar sobre los riesgos en la utilización de internet, con respecto al manejo de datos personales, violación a los derechos de imagen e intimidad y los delitos informáticos como pornografía infantil, hostigamiento o ciberbullying, el acoso sexual y el llamado cibergrooming, donde las víctimas resultan ser los niños, niñas y adolescentes.

En el marco de este proyecto se dió lugar al Trabajo Social Obligatorio de la carrera de Abogacía, denominado *Conexión Segura*, en el cual un grupo de estudiantes dirigidos por el equipo docente de la asignatura, llevaron a cabo las capacitaciones y campañas de concientización a docentes y estudiantes secundarios sobre diferentes aspectos vinculados al Derecho Informático, principalmente de delitos informáticos y protección de datos personales.

Como actividad investigativa, los y las estudiantes han desarrollado múltiples trabajos finales de grado propios en referencia a las temáticas trabajadas en la asignatura de Derecho Informático, algunas vinculadas con los ciberdelitos, ya sea trabajando sobre alguno en particular o en general. Asimismo se han presentado trabajos vinculados a los aspectos legales del uso de las redes sociales, elaborando tesis enmarcadas en cuestiones de privacidad, protección de datos personales y propiedad intelectual.

CONCLUSIÓN

Encontrándonos inmersos en la sociedad de la información no se ha podido desconocer la necesidad de incorporar la materia de Derecho Informático como

asignatura obligatoria dentro del plan de estudios de la carrera de abogacía de la Universidad Nacional de Río Negro.

Se ha elaborado un programa analítico que busque abarcar los conceptos generales y particulares vinculados a los derechos y la implementación de las nuevas tecnologías de la información y la comunicación. Tratando de desarrollar a través de distintas metodologías de estudios, capacidad analítica y crítica de los y las estudiantes, generando que en el ejercicio de la actividad profesional se encuentren preparados para enfrentarse a la realidad de la que ya son parte.

La implementación de esta asignatura ha despertado interés tanto en los docentes como en los estudiantes, generando de esta manera un caudal de proyectos de investigación personales y grupales, que desde su lugar buscaron como objetivo final contribuir al desarrollo de la formación propia y en algunos casos de la sociedad misma, en temáticas novedosas pero esenciales para desarrollarse en la realidad actual.

El derecho informático empuja a docentes e investigadores a adaptarse a una dinámica de conocimiento en continuo movimiento y actualización, por lo que el contenido planteado siempre se encuentra pendiente de actualización y

las investigaciones en curso son solo el principio de todo lo que irá a venir en el futuro. Pero lo que se creía lejano ya ha llegado, y en ese sentido el desafío será adaptarse lo más pronto posible a la realidad.-

Responsabilidad". Secretaría de Políticas Universitarias, Ministerio de Educación de la Nación. Universidad Nacional de Río Negro. 2016.

BIBLIOGRAFÍA

- Beca Estimulo a las Vocaciones Científicas. Consejo Interuniversitario Nacional. Proyecto: "El Derecho Penal y la Protección de Menores en Internet". Director: Dr. Fernando Barrio. 2015-2016.
- Lambrecht, A. "El Estado como Usuario de Redes Sociales". Trabajo Final de Grado. Universidad Nacional de Río Negro. 2016.
- Plan de Estudios. Carrera Abogacía. Universidad Nacional de Río Negro - Sede Atlántica.-
- Programa Analítico Asignatura Derecho Informático. Carrera Abogacía. Universidad Nacional de Río Negro - Sede Atlántica.
- Proyecto de Investigación "El Derecho Penal y la protección de menores en Internet". Universidad Nacional de Río Negro. 2015.
- Proyecto de Voluntariado Universitario "Conectando con

¿SON LAS NUEVAS TECNOLOGÍAS UNA NUEVA FORMA DE VER, ENTENDER Y ENSEÑAR EL DERECHO?¹⁶⁰

Fernando O. Branciforte¹⁶¹

RESUMEN:

No cabe ninguna duda que la pandemia que aqueja al mundo ha cambiado la vida de toda la población, llevándola a una digitalización obligatoria.

Sin embargo, esta “actualización” en nuestras formas de relacionarnos social y jurídicamente, ya se venía gestando hace varios años, incluso me atrevo a decir que desde el nacimiento de Internet.

De este modo, la digitalización y las tecnologías que fueron naciendo llevaron a nuevas formas de relacionarnos y con ello a nuevas relaciones jurídicas.

Es en este punto donde con el presente trabajo intentaremos analizar que entendemos por Nuevas Tecnologías y si las mismas influyen en nuestro ordenamiento legal tanto a la hora de entender el mismo y aplicarlo, así como de enseñarlo a futuras generaciones de legos.

Asimismo y siguiendo con éste pensamiento analizaremos si la figura del abogado actual inclinado hacia el estudio de las Nuevas Tecnologías es diferente a la figura del abogado tradicional.

PALABRAS CLAVE: digitalización, nuevas tecnologías, pandemia

160 Enlace al video <https://youtu.be/fUfTsNQtMOA>

161 Abogado (UNS). Director del Instituto de Derecho Informático y TICS del CABB, Vocal del Instituto de Derecho de los Consumidores y Usuarios del CABB, Consultor y Socio Mail de contacto: estudiobyb@speedy.com.ar.

¿QUÉ SON LAS NUEVAS TECNOLOGÍAS?

Previo a comenzar a desarrollar el análisis completo del presente trabajo es necesario que establezcamos qué entendemos por Nuevas Tecnologías.

Cuando hacemos alusión al término Nuevas Tecnologías nos referimos a aquellas nuevas técnicas que han surgido y van surgiendo a lo largo de los años para facilitar y mejorar las comunicaciones y la información así como también las finanzas y economía mundial.

De este modo, el término Nuevas Tecnologías lo aplicamos de manera genérica no limitándonos solamente a las TICs.

Es que, con el paso de los años, las tecnologías han logrado una expansión tal que no podemos limitarlas a sistemas de comunicación o información, sino que hoy en día ya son utilizados también para interactuar en sistemas financieros propios y hasta “creando dinero”.¹⁶²

En este sentido, vemos también que cuando hablamos de Nuevas Tecnologías no sólo hablamos de hardware sino también del software y de ambos componentes actuando como uno solo.

¹⁶² Un claro ejemplo de esto son las criptomonedas y los sistemas DeFi actuales.

De aquel Internet original nacido aproximadamente en el año 1983 ya poco queda, el mismo ha ido evolucionando permitiendo cada vez mayor participación del ser humano a tal punto que nuevos sistemas han sido elaborados encontrándonos actualmente en lo que la gran mayoría de los autores reconocen como la Revolución Industrial 4.0, cuyo punto de inflexión en la gestación de la tecnología Blockchain y de la Inteligencia Artificial.

Ahora bien, la frase “Nuevas Tecnologías” incluye la palabra “nuevas” es decir, algo novedoso, actual, pero aquí debemos preguntarnos cuando se adquiere ese carácter de novedad y, por el contrario, cuando se pierde la misma.

Como dijimos antes, Internet ya no es una nueva tecnología, la misma ya ha sido aprendida y adaptada por muchos. Por el contrario, la Inteligencia Artificial, los sistemas DLT como la tecnología Blockchain y sus derivados, si pueden considerarse Nuevas Tecnologías.

Entonces ¿cuál es el parámetro para considerar a alguna tecnología como nueva tecnología? Entendemos que el parámetro temporal es fundamental y dicho parámetro viene de la mano del desarrollo de la tecnología, cuando la misma aún no alcanzó toda su

potencialidad, pero adquirió una masificación en su utilización, en ese caso podemos hablar de que esa tecnología es novedosa, es en este caso donde consideramos que nos encontraríamos frente a una Nueva Tecnología.

SU INFLUENCIA EN EL DERECHO

Teniendo el concepto de Nuevas Tecnologías, no podemos negar que las mismas tienen relación con el Derecho. Una prueba cabal de ella es el presente artículo así como los diversos congresos o eventos que se realizan.

La pregunta por la que debemos iniciar es si son las tecnologías las que influyen en el Derecho o es el Derecho el que influye en las tecnologías.

El objetivo del presente análisis es demostrar también que la influencia está en ambos sentidos.

Desde el punto de vista de las nuevas tecnologías las mismas llegaron para quedarse y poder ser utilizadas como herramientas que mejoren los procesos.

En este sentido, la pandemia llevó a una “digitalización obligatoria” en todos los aspectos de la vida pública y privada.

Así las cosas, las nuevas tecnologías aparecen como herramientas que ayudan

a la digitalización en estos nuevos tiempos.

Claros ejemplos de ello son el expediente digital, la aplicación de inteligencia artificial a la hora de facilitar resoluciones¹⁶³, el teletrabajo, la firma digital¹⁶⁴ y electrónica, las notificaciones electrónicas, las notificaciones en carta documento con código qr¹⁶⁵, entre otras.

Desde la vereda de enfrente vemos también como las Nuevas Tecnologías deben adaptarse al Derecho y a su normativa.

Un ejemplo de ello es el teletrabajo nombrado en párrafos superiores como una forma de llevar adelante trabajos en tiempos de pandemia y que, al ser regulado recientemente, también deberá adaptarse al Derecho actual.

En esta doble relación entre las Nuevas Tecnologías y el Derecho, también debemos considerar las nuevas formas de llevar adelante las contrataciones en el mundo de la economía, negocios y finanzas con el mayor desarrollo de las

163 Caso Prometea

164 Aquí es dable aclarar que la firma digital no debiera ser considerada una Nueva Tecnología por cuanto su ley ya lleva más de 20 años entre nosotros aunque recién en este último tiempo comenzó a masificarse su uso.

165 vgr. Juzgado Civil y Comercial N° 1 de La Plata, en causa «Cerezo Mirta Noemí c/ Instituto de obra Médico Asistencial de la Provincia de Bs. As. s/ Desalojo» N° 888906

Fintech, la masificación y nuevas formas de llevar adelante el crowdfunding o el crowdlending, las contrataciones por medio de plataformas online, los nuevos medios de intercambio de valor como las criptomonedas, las nuevas formas de inversión como los sistemas DeFi.

Todos los ejemplos nombrados en estos párrafos también tuvieron su intervención desde el lado del derecho, como para nombrar algunos ejemplos podemos hacer referencia a la ley de crowdfunding y la normativa de la CNV en su influencia con sistemas ya vigentes como el caso de la plataforma de inversiones SeSocio.com que debió readaptarse a la normativa vigente para poder continuar con la operatoria de la plataforma.

En igual sentido la normativa del BCRA¹⁶⁶ respecto al funcionamiento de los PSP (Proveedores de Servicios de Pago), en conjunto con normativa de la AFIP-DGI¹⁶⁷ aplicable a los criptoactivos y los Exchanges.

De este modo, vemos como el Derecho también influye en las Nuevas Tecnologías a través del marco regulatorio que conlleva a que las mismas se adapten a las normas vigentes.

166 Comunicaciones "A" 6823, "A" 6859 y "A" 6885

167 Reg.Gral 4614 e incorporación de los criptoactivos al régimen del impuesto a las ganancias.

¿UNA NUEVA FORMA DE ANALIZAR Y TRANSMITIR EL DERECHO?

Ahora bien, en este doble camino de influencia entre el Derecho y las Nuevas Tecnologías aparecemos los operadores del derecho como medios que analizan y deben transmitir el mismo a futuras generaciones, y en consecuencia, también nos vemos influenciados por estos avances novedosos.

Es que ya no basta con aprender, analizar y enseñar como es un contrato (por ejemplo de compraventa) sino que también, hoy en día, hace falta aprender, analizar y enseñar en qué medio se realizó ese contrato (plataforma online, de manera virtual, digital, por Smart Contracts) así cómo cual es el objeto del mismo (ejemplo criptomonedas o tokens) y la tecnología utilizada de trasfondo (inteligencia artificial, blockchain).

Así vemos, que como operadores del Derecho, en la realidad actual, también debemos saber del funcionamiento de estas tecnologías, debemos ingresar a un ámbito más técnico sobre cada operación, y hasta comenzar a trabajar en conjunto con otras ciencias pero, nuevamente, para ello debemos estudiar cómo funcionan estas nuevas tecnologías y así también aprender otras terminologías y

herramientas que van más allá del Derecho.

Y esto mismo se replica hacia los docentes que enseñan y enseñarán sobre estas Nuevas Tecnologías, será necesario aprender la parte técnica y su funcionamiento para luego replicarla a los alumnos previo a entrar en la fase legal.

De este modo, a mi entender, la docencia actual del Derecho (en aquellos aspectos más influenciados por las Nuevas Tecnologías) debiera constar de tres etapas:

- Etapa Técnica: Donde explicar la tecnología subyacente, cómo se creó la misma, cómo funciona y cuál es su objetivo;
- Etapa Legal: Donde desarrollar la normativa aplicable a la misma;
- Etapa Práctica: Donde podamos ver y enseñar cómo esta nueva tecnología es una nueva herramienta para nuestro accionar diario.

CONCLUSIÓN

Como conclusión del presente artículo podemos decir que del desarrollo aquí brevemente analizado, hoy nos encontramos ante un nuevo mundo legal que influye y, a su vez, es influenciado por las Nuevas Tecnologías.

En este nuevo mundo legal tecnológico, los operadores del derecho deben aprender a convivir con estas nuevas herramientas pero, para ello, deberán aprender cómo funcionan para luego poder analizar que normativa es aplicable a la misma. Y, este mismo razonamiento, deberá ser transmitido a las nuevas generaciones por medio de una enseñanza completa que no solo abarque la parte legal sino que también incluya la parte técnica de las nuevas tecnologías así como su faz práctica.

Finalmente, estamos viendo la aparición y la gestación de un nuevo perfil de abogado más intuitivo con la tecnología, ágil a la hora de utilizar las mismas y que también entiende y entenderá cada vez con más detalles cómo funciona la misma. Así las cosas, la tecnología avanza y es nuestro deber estar a su ritmo actualizándonos en nuestros conocimientos y en nuestro ser.

LA ENSEÑANZA DEL DERECHO EN FORMA VIRTUAL: DESCRIPCIÓN Y ANÁLISIS DE LO SUCEDIDO DURANTE LA PANDEMIA ¹⁶⁸

Marcos Fernández Peña¹⁶⁹

Martina Santillán¹⁷⁰

RESUMEN

Dado que las nuevas tecnologías en el contexto del siglo XXI se han masificado y forman parte de la vida diaria, éstas ingresaron en las instituciones educativas, con o sin el consentimiento formal de sus autoridades. El Departamento de Derecho de la Universidad Nacional del Sur no fue ajeno a esa dinámica. En este sentido, si bien se incorporaron algunas herramientas virtuales en el proceso educativo, la presencialidad fue siempre entendida como un aspecto irremplazable en la formación de los estudiantes. Sin embargo, el advenimiento de la crisis sanitaria implicó la subversión de ese paradigma, imponiéndose la virtualidad como el medio exclusivo a través del cual se produce la enseñanza. En este trabajo describiremos los resultados que se obtuvieron en una encuesta realizada a los alumnos, relativa a su percepción respecto de varios de los aspectos que acarrió este nuevo modo de aprendizaje en el marco de la pandemia.

PALABRAS CLAVE: nuevas tecnologías, enseñanza, crisis sanitaria

168 Enlace al video: https://youtu.be/ucPY5Rxi_XQ

169 Abogado y Maestrando en Políticas y Estrategias en la Universidad Nacional del Sur. Miembro del Proyecto de Investigación “Desafíos de la Enseñanza del Derecho en el Siglo XXI: la inserción de las prácticas jurídicas en los planes de estudio de las universidades nacionales”. Correo electrónico: fernandezmarc@hotmail.com.ar.

170 Abogada. Miembro del Proyecto de Investigación “Desafíos de la Enseñanza del Derecho en el Siglo XXI: la inserción de las prácticas jurídicas en los planes de estudio de las universidades nacionales”. Correo electrónico: martinasantillan.uns@gmail.com.

INTRODUCCIÓN

La infraestructura edilicia de la Universidad Nacional del Sur (UNS) y la cantidad de alumnos presentes en los cursos de su Departamento de Derecho, trajeron como consecuencia que las decisiones de los profesores respecto al método de dictado de clases, estuvieran basados más en lo *posible* -en lo que las circunstancias admitieran como de realización factible- que en lo *ideal*.

En este sentido, se acudió mayoritariamente a la denominada “clase magistral” en la cual el profesor expone a los futuros abogados las regulaciones que forman el sistema y éstos deben reproducirlas fielmente en los exámenes. Este modo de enseñanza, si bien ha sido criticado por diversos autores¹⁷¹, presenta algunas ventajas¹⁷²: es eficaz para asegurar una visión global de la lógica de la disciplina y es uno de los métodos más económicos, puesto que se puede preparar rápidamente y repetir indefinidamente a un gran número de alumnos.

171 Frondizi (1971) afirma que el curso panorámico está condenado, por su extensión, a ser superficial e informativo y que los cursos generales de tipo informativo tienen un bajo índice de transferencia. En el mismo sentido, el célebre profesor Jean Buguet llegó a afirmar “No conozco el derecho civil. Sólo enseñé el Código de Napoleón”.

172 Señaladas por Campari (2005).

En cuanto a las nuevas tecnologías, su introducción quedó librada a la voluntad de los docentes a cargo de las materias, pero la presencialidad siempre fue entendida como indispensable para un tránsito universitario exitoso. En esta sintonía, si bien la Universidad provee a todos los Departamentos de la plataforma virtual Moodle para el intercambio virtual entre docentes y alumnos, hasta inicios de 2020 eran los profesores los que decidían si, cómo y qué de esa plataforma utilizarían.

El contexto descrito en los dos párrafos anteriores se vio modificado súbitamente por el advenimiento de la crisis sanitaria, que cambió no sólo el método de dictado de clases sino la forma misma de interrelación entre docentes y alumnos y hasta el acceso a la bibliografía. Todos los profesores debieron implementar, en algún grado, la tecnología para el dictado de clases; la plataforma Moodle, pasó a ser el canal principal de comunicación de contenidos y de intercambio entre profesores y alumnos, y otras herramientas audiovisuales -como las videollamadas para realizar los exámenes finales- se erigieron como instrumentos indispensables para el cursado.

En este breve trabajo, expondremos algunos resultados de una encuesta

realizada¹⁷³ a 845 alumnos de la carrera de Abogacía de la UNS, efectuada con el fin de evaluar el impacto que ha tenido la pandemia en la enseñanza, y cómo y en qué aspectos se han introducido las nuevas tecnologías.

I. RESULTADOS DE LA ENCUESTA.

La encuesta fue realizada sobre tres grandes ejes: a) Enseñanza Práctica del Derecho; b) Relación Docente-Estudiante / Relación entre pares c) Experiencias personales.

a. Enseñanza Práctica del Derecho.

El Departamento de Derecho de la UNS puso en vigencia en 2020 el Nuevo Plan de Estudio de la carrera de Abogacía, que integra la enseñanza teórica con la enseñanza práctica del Derecho. En concreto, incorpora mayor carga horaria de práctica en las todas las asignaturas y crea talleres con el objetivo de transmitir destrezas indispensables para el ejercicio profesional. En consecuencia, uno de los grandes desafíos que planteó la virtualidad fue la formación práctica de los

estudiantes a través de las plataformas digitales.

En este orden de ideas, al ser consultados sobre su percepción respecto a las actividades prácticas desarrolladas en la Cátedra Virtual, el 55,7% de los encuestados contestó que ésta había sido “suficiente”, mientras que el 28,9% respondió que la misma había sido “insuficiente”, y el 15,4% manifestó no haber recibido formación práctica durante el cursado virtual. Es decir, casi la mitad de los encuestados (44.3%), manifestaron no haber obtenido una formación práctica satisfactoria.

Dentro de los que manifestaron tener algún grado de enseñanza práctica, se les consultó si la modalidad adoptada les había permitido comprender mejor los conocimientos teóricos. Los resultados en este sentido fueron particulares: 506 expresaron que la modalidad adoptada les permitió comprender mejor el tema (trasladar la teoría a la ejercitación práctica o aprender de otro modo que no sea la simple lectura); sin embargo, más de un cuarto de los encuestados -222 alumnos, el 26,6%- dijeron que la modalidad adoptada no les aportó nada.

¹⁷³ A fines del primer cuatrimestre de 2020.

b. Relación docente- estudiante y Relación entre pares.

Como sostuvimos al inicio, el vínculo docente-alumno y la relación entre pares, también fueron súbitamente modificados, en tanto las relaciones interpersonales en pandemia se producen en diferentes tiempos y/o espacios.

En este sentido, se preguntó a los alumnos cómo consideraron que había sido la relación con los docentes. Los estudiantes contestaron que ésta fue: “muy buena” (31,8%), “buena” (26,7%), “regular” (14,8%); “mala” (10,8%) y, en algunos supuestos, “inexistente” (15,9%).

Siguiendo en la línea de evaluar la relación interpersonal, se les preguntó si habían utilizado los canales de consulta habilitados por las Cátedras Virtuales, y en caso afirmativo, si habían recibido respuestas en un plazo prudencial. Del cuestionario surge que aproximadamente 500 estudiantes habían utilizado, al menos una vez, las vías facilitadas por la Cátedra para hacer preguntas, y, de ellos, 353 recibieron la respuesta en un plazo razonable. Sin embargo, 81 recibieron respuestas, pero en forma tardía y, el resto directamente no recibió respuesta alguna.

Finalmente, 339 alumnos consideraron que la comunicación con los profesores

fue uno de los obstáculos más relevantes que experimentaron durante el desarrollo de la cursada virtual. Teniendo en cuenta que ese universo representa el 40% de los encuestados, es un dato no menor al hacer un análisis cualitativo del cursado virtual hacia el futuro.

Por otra parte, dado que la enseñanza es un proceso social y que toda la doctrina pedagógica es conteste en señalar los beneficios de la socialización en el proceso de aprendizaje, es preocupante el dato obtenido en torno a la relación entre pares. En este sentido, 396 alumnos respondieron que nunca habían estudiado / trabajado en grupo, 356 respondieron que lo hicieron “a veces” y sólo 96 encuestados respondieron que lo hicieron “siempre”.

c.

No obstante lo expresado con anterioridad, pareciera ser que la mayoría de los encuestados converge en señalar que los beneficios de la virtualidad han superado a las dificultades. Así, más del 60% calificó su experiencia durante la cursada virtual en forma positiva - “Muy buena” el 29,6% y “Buena” el 32,7%-mientras que sólo el 37,7% la calificó de “Regular” (18,3%) o “Mala” (19,4%).

En esta misma línea, al ser preguntados sobre cómo pretendían que sea la

cursada en el futuro, más de la mitad (el 54,6%) respondió que se deberían combinar ambos sistemas (clases presenciales y virtuales), sólo el 32,2 % optó que se vuelva al sistema anterior (clases presenciales) y el 13,2% restante prefiere que se mantenga el sistema exclusivo de clases virtuales.

CONCLUSIÓN

En función de los datos obtenidos en la encuesta, es posible concluir que el Departamento de Derecho de la UNS ha obtenido cierto éxito en lograr mantener el dictado de la currícula en la emergencia sanitaria. En este sentido, ha podido dictar todas las materias del cuatrimestre y se ha adaptado a la virtualidad, supliendo los modos de tradicionales de dictado de clases.

Sin embargo, hemos visto que hubo importantes deficiencias en la efectiva evacuación de consultas, la formación práctica y la socialización entre pares. Por ese motivo, debe propenderse a realizar las modificaciones necesarias para que el proceso de aprendizaje a través de las Plataformas Virtuales, se ajuste a las necesidades humanas. Si es una posibilidad que la semi-presencialidad se imponga en la pospandemia (como más de la mitad de los estudiantes lo

demandan) se debe trabajar sobre ese aspecto.

No hay que olvidar que, en definitiva, cualquier tecnología que se aplique a la enseñanza no es un fin en sí misma, sino un medio para producir el fenómeno educativo. Si le falta el aspecto vincular y práctico, se afectará una parte de la excelencia académica que siempre ha caracterizado al Departamento de Derecho de la Universidad Nacional del Sur.

REFERENCIAS BIBLIOGRÁFICAS

- CAMPARI, S. (2005). "Enseñar Derecho pensando en el profesional del Siglo XXI", en *Academia: Revista sobre enseñanza del derecho de la Universidad de Buenos Aires*, Año 3, Número 5, pp.185-200.

- FRONDIZI, R. (1971). *La Universidad en un Mundo de Tensiones*, Buenos Aires, Paidós.

Encuesta realizada por el Proyecto Grupo de Investigación "Desafíos de la Enseñanza del Derecho en el Siglo XXI: la inserción de las prácticas jurídicas en los planes de estudio de las universidades nacionales" resultados disponibles en https://docs.google.com/forms/d/17wK5ipNj5Pis1WwXZ-gcqywjDM42ApbW9Tghhjzq2Ew/edit?usp=sharing_eip&ts=5f84b54c.

Capítulo 6

La Tecnología en la Investigación y en la Experiencia Práctica

EL CATÁLOGO DE DERECHOS DIGITALES EN LA LEGISLACIÓN ESPAÑOLA Y EUROPEA¹⁷⁴

Wilma Arellano Toledo¹⁷⁵

RESUMEN¹⁷⁶:

Los derechos fundamentales se hallan garantizados por distintos instrumentos internacionales de derechos humanos y, en principio, su aplicación es universal y no depende los medios o entornos en donde deban ser protegidos.

Sin embargo, tanto doctrinal como legalmente se ha considerado necesario configurar una serie de derechos que tienen relación directa con el ámbito digital y que, evidentemente, no fueron integrados en Declaraciones o Convenios de derechos humanos por la época en la que fueron aprobados y ratificados. Estos nuevos derechos digitales, vendrían a complementar a los derechos humanos ya reconocidos en el terreno de los tratados internacionales y en los distintos textos constitucionales de los países, mismos que se reconocen y respetar también en el espacio online.

Los derechos digitales son diversos y en este documento mencionaremos cada uno de ellos, pero pondremos especial atención a aquellos que tienen un vínculo intrínseco con el derecho a la intimidad, a la privacidad y a la protección de los datos de carácter personal; puesto que son los que mayor desarrollo legal han tenido.

174 Enlace al video <https://youtu.be/A8N90-9LlgU>

175 Doctora por la Universidad Complutense de Madrid. Especialista en Derecho de las TIC y de la Información y privacidad en el entorno digital. Miembro de OdiselA (Observatorio de Impacto Social y Ético de la Inteligencia Artificial) y del Observatorio de la Transformación Digital del Sector Público de la Cátedra PAGODA de Gobierno Abierto, Participación y Open Data.

176 Artículo realizado en el marco del Proyecto de I+D+i Retos MICINN “Derechos y garantías frente a las decisiones automatizadas en entornos de inteligencia artificial, IoT, big data y robótica” (PID2019-108710RB-I00, 2020-2022), financiado por el Ministerio de Ciencia e Innovación de España y del cual forma parte la autora.

PALABRAS CLAVE: *derechos fundamentales, ámbito digital, derecho a la intimidad, a la privacidad y a la protección de los datos de carácter personal*

SOBRE LOS NUEVOS DERECHOS DIGITALES EN LA NORMATIVA EUROPEA

La Unión Europea se ha caracterizado por ser una región del mundo con gran tradición en la protección de los derechos humanos (sobre todo en los de primera y segunda generación), tras las experiencias vividas por las guerras y las dictaduras en varios países. En materia de privacidad y protección de datos personales (que forman parte de la tercera generación de derechos), las Directivas europeas han sido siempre muy estrictas en cuanto a la observancia de principios y de derechos de los titulares de los datos. Y, el actual Reglamento General de Protección de Datos -RGPD¹⁷⁷- (que tiene aplicación directa en todos los países miembros) no es menos severo en ese sentido¹⁷⁸.

177 Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

178 Incluso, hay quien sostiene que “la normativa de la Unión Europea en el campo de la protección de datos es la más exigente del planeta” y puesto que hay países en donde sucede todo lo contrario

El RGPD fue aprobado en 2016 y entró en vigor, tras una *vacatio legis*, en 2018. Contiene una serie de disposiciones que adaptan la anterior Directiva 95/46 de protección de datos a la realidad actual en cuanto al tratamiento de datos y tomando en consideración el papel de las Tecnologías de la Información y la Comunicación (TIC). Es en este contexto que nacen una serie de derechos que se han denominado derechos digitales, pues son concebidos para ser ejercidos por los titulares en los medios digitales, Internet, aplicaciones móviles y un sinnúmero de dispositivos conectados (incluyendo los del Internet de las Cosas¹⁷⁹). La razón de que se hayan reconocido y se empiecen a configurar como derechos de mayor alcance es que “resulta incuestionable que la sociedad contemporánea afronta el reto mayúsculo de constitucionalizar nuevos derechos que satisfagan la demanda social de protección frente a

“se han regulado minuciosamente las transferencias internacionales de datos” (Guash Portas, 2012: 415).

179 Para abundar en este tema, también denominado Internet de los Objetos se puede consultar Arellano, 2017.

riesgos y amenazas presentes y futuras” (Rallo, 2017: 642).

Es por eso que el RGPD hace un reconocimiento a derechos relacionados con los usos de Internet y el ciberespacio, pero también con referencia al Big Data, al uso de algoritmos y a la Inteligencia Artificial. Como premisa, se tiene en cuenta la neutralidad tecnológica para la garantía de los derechos digitales, puesto que se persigue “evitar que haya un grave riesgo de elusión” y así “la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas”, según se expresa en el Considerando 15.

Los derechos de los interesados que se consagran en este texto legal se corresponden en buena medida con aquellos que ya estaban definidos en la Directiva 95/46 que le precede. Se resumen en el derecho a la transparencia en el manejo de datos personales, el derecho a ser informados sobre el tratamiento y finalidad de los datos y los derechos ARCO¹⁸⁰ o la comunicación de brechas de seguridad, por mencionar sólo algunos.

180 Como se sabe, el acrónimo se refiere a los derechos de acceso, rectificación, cancelación y oposición al tratamiento de nuestros datos personales.

De estos derechos ARCO, destaca el derecho de supresión, que el RGPD ya denomina claramente como “derecho al olvido”, tras la jurisprudencia europea al respecto y que ha sido conocida mundialmente. Este derecho al olvido, implica que en determinadas situaciones el “interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernen, el cual estará obligado a suprimir sin dilación indebida los datos personales”¹⁸¹.

Entre las novedades que introduce este Reglamento (vinculante para todos los Estados miembros) está la de reconocer un derecho específico para los menores de edad, en cuanto al consentimiento

181 Los supuestos en torno a los cuales se puede ejercer del derecho al olvido, de acuerdo con lo estipulado en el artículo 17 del RGPD, implican que ocurra una de las siguientes situaciones: “a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1”.

para hacer lícito un tratamiento de datos personales. En el artículo 8 se explica que “el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño”.

Otro de los derechos introducidos en este ordenamiento es el que tiene que ver con la portabilidad de los datos personales, pues se establece que el titular de los mismos tendrá derecho a recibirlos de manos de aquel responsable al que se los haya proporcionado. Este derecho implica que el “interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica”.

Ahora bien, como ya hemos adelantado, en este Reglamento Europeo se contemplan unos derechos que tienen que ver con el Big Data, la IA y el uso de algoritmos para la toma de decisiones. En este sentido, se trata de empoderar al individuo para que tenga la posibilidad de oponerse a ser objeto de dichas decisiones, basadas en procesos

automatizados. El artículo 22 expone claramente que “todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar”. Esto sin duda, es un avance importante, puesto que de algún modo otorga una libertad frente al algoritmo, o una especie de autodeterminación ante el algoritmo¹⁸².

Por otro lado, uno de los asuntos en los que ha insistido la Comunidad Europea en los últimos años, es el que tiene relación la privacidad desde el diseño y la privacidad por defecto. Desde que el primero de éstos conceptos fuera planteado por la Comisionada de Privacidad de Ontario, Ann Cavoukian, se ha colocado en el centro del debate como una de las soluciones para garantizar una protección al derecho a la intimidad, sobre todo en cuanto al uso de dispositivos electrónicos. Estos principios de privacidad desde el diseño y privacidad por defecto, implican que los

182 En cuanto a estos planteamientos, es muy interesante revisar el Dictamen del Supervisor Europeo de Protección de Datos sobre «Hacer frente a los desafíos que se plantean en relación con los macrodatos: llamamiento a la transparencia, el control por parte de los usuarios, la protección de datos desde el diseño y la rendición de cuentas».

responsables del tratamiento de datos personales apliquen técnicas de anonimización¹⁸³ y de minimización de datos¹⁸⁴. La idea, es “garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento”.

LOS NUEVOS DERECHOS DIGITALES EN LA NORMATIVA ESPAÑOLA

Ahora bien, como ya se ha dicho, el Reglamento es vinculante para todos los Estados miembros, pero aún así, en España se ha hecho la transposición a la norma interna de sus preceptos, vía la Ley de Protección de Datos y Derechos

183 Sobre estas técnicas y sobre la necesidad de no confundirlas con pseudoanonimización, es muy recomendable el Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del Artículo 29, adoptado el 10 de abril de 2014.

184 En el Reglamento, el artículo 25.1 es claro cuando ordena que “1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados”.

Digitales (LOPDDD) de 2018¹⁸⁵ que sustituye a la LOPD de 1999¹⁸⁶.

Es el Título X de la nueva LOPDDD la que establece una serie de derechos digitales y dedica todo el apartado a este asunto. Como premisa fundamental y haciéndolo al modo en que lo haría un precepto constitucional, se define que todos aquellos derechos expresados en la Constitución y en los Tratados e instrumentos internacionales de derechos humanos de los que España sea parte “son plenamente aplicables a Internet” (artículo 79). Son los prestadores de servicios de la Sociedad de la Información y los proveedores de Internet los que deben contribuir a garantizar su aplicación, aunque en toda regla, sean los poderes públicos facultados para ello, los que tienen como atribución esencial garantizarlos para los individuos¹⁸⁷, sujetos de derechos fundamentales.

Para que se puedan ejercer los derechos digitales, tiene que haber otra premisa y

185 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

186 Nos referimos a la La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que estuvo vigente casi una veintena de años en España.

187 Por ejemplo, la Agencia Española de Protección de Datos o el Consejo de Transparencia y Buen Gobierno, así como los organismos de las autonomías.

es el acceso a los medios tecnológicos adecuados. De este modo, el artículo 81 viene a establecer un derecho de acceso a Internet que si bien, está ligado al de servicio universal de telecomunicaciones ya garantizado por la Ley General de Telecomunicaciones de 2014 y que no aparece en la Constitución de 1978 por obvias razones¹⁸⁸, incorpora un nuevo contenido y alcances, puesto que no se limita al contenido clásico de asequibilidad, accesibilidad y calidad, sino que ahonda en características como las de brecha de género, de edad, de la dicotomía ciudad-entorno rural y en relación con las personas con capacidades diferentes.

Al igual que hace el Reglamento Europeo, en la legislación española se considera importante establecer otro presupuesto para luego describir una serie de derechos digitales y nos referimos al derecho a la neutralidad de Internet.

188 Aunque la Constitución Española se redactó con una cierta visión moderna al introducir conceptos como el de la informática, es verdad que en los años setenta no existían ni las redes de telecomunicaciones actuales ni el Internet que conocemos hoy en día. Sobre esto, tenemos que “La meritoria —por expresa y vanguardista— referencia a la *informática* en el texto constitucional de 1978 constituyó un innegable aldabonazo para otorgar trascendencia constitucional a la necesaria protección del individuo frente a los riesgos que sobre él —y, particularmente, sobre el disfrute de algunos de sus derechos fundamentales— cernían los avances tecnológicos ligados a la incipiente y primaria computerización” (Rallo, 2017: 642).

Mucho se ha discutido sobre este particular en los foros internacionales y particularmente en los que habla de gobernanza en la Red. Específicamente, este derecho implica que “los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos”.

Otra premisa que es muy importante para ejercer los derechos digitales es, además del acceso, la apropiación de la tecnología. Y en este sentido, el legislador ha querido integrar a la LOPDDD el derecho a la educación digital, derecho que incluso podría estar ligado al que hemos defendido como derecho a la transparencia algorítmica en la era del Big Data y la Inteligencia Artificial (Arellano, 2017). Esto es así, porque el derecho a la transparencia algorítmica implica el conocimiento por parte de los individuos de la lógica aplicada en el Big Data y la IA cuando se tomen decisiones que le puedan afectar. Pero entender esa lógica implica, evidentemente, unas cualificaciones.

Este derecho a la educación digital mencionado en la LOPDDD, implicaría

dichas cualificaciones y también unas herramientas para los usuarios frente -por ejemplo- a la desinformación, dado que las “fake news” triunfan en tanto sean consumidas y se les otorgue credibilidad. Y para que “triunfen” es necesario que los usuarios contribuyan, por lo que es importante destacar la responsabilidad que éstos tienen, y la necesidad de ética empresarial, pero también de una autorregulación social. El derecho a la educación digital les aportaría muchas de esas herramientas, puesto que no sólo hace falta enseñar cómo usar una TIC, sino confluir en una auténtica apropiación de la tecnología.

El artículo 85 expone con claridad que todas las personas tienen derecho a la libertad de expresión en Internet. Cosa que, por otro lado, no podría ser de otra forma dada la interpretación del artículo 20 de la Constitución, que establece unas facultades de investigar y difundir información “por cualquier medio”¹⁸⁹.

189 En concreto, el literal constitucional expresa que “1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. c) A la libertad de cátedra. d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades” (las cursivas son nuestras).

En el mismo literal, se habla de un derecho de rectificación ante informaciones que puedan ser vertidas en las redes sociales y que atenten contra un derecho al honor. El alcance y objeto de la Ley implican un reconocimiento de ese derecho de rectificación que está primordialmente enfocado al honor y a la privacidad, pero que también puede plantearse en relación a la desinformación, cuando se explica que “los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos [que atenten contra] el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación”.

En la Ley de Protección de Datos española, al igual que en el RGPD, el artículo 93 vuelve sobre un tema sobre el que ya se había pronunciado el Tribunal de Justicia de la Unión Europea y es aquel que se refiere al derecho al olvido. Se especifica que se refiere a los motores de búsqueda de Internet y aquí, quizá sería interesante pensar cómo una fórmula similar podría aplicarse a aquellas

“noticias falsas” o fenómenos de desinformación. Porque claro, no siempre se sentencia que en esos casos se trate de fake news y en los casos en que esto se hace evidente, la “información” continúa en las redes, dejando un rastro permanente de datos erróneos, sesgados o francamente falsos, quizá para siempre. Sería importante pensar en qué caminos, por lo menos, de desindexación, como sucede con el derecho al olvido y de borrado permanente, son necesarios tras la publicación de “noticias” que puedan afectar en los momentos en los que se emiten y en momentos futuros¹⁹⁰. Por ejemplo, en aquellos casos en los que afectan un proceso electoral, podrían afectar a otros procesos futuros si permanecen en las redes aún sabiendo que se trata de falsedades, pero que puede que un lector-usuario-consumidor pueda leer en un futuro sin saber que lo son¹⁹¹.

Pero en el ámbito personal, este derecho al olvido se complementa con lo dispuesto en el artículo 86 sobre un derecho a la actualización de informaciones en

medios de comunicación digitales, que supondría que “toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernen cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio¹⁹²”. Estaríamos hablando de un complemento también al derecho de información que forma parte de los principios rectores en materia de protección de datos de carácter personal.

También sobre derecho al olvido, la Ley española establece un contenido que va más allá del del Reglamento de Europa, puesto que no se refiere únicamente a la desindexación de informaciones de los

190 Y esto es particularmente importante porque como ha dicho John Cook (un psicólogo que investiga la desinformación), el gran peligro de la desinformación no sólo es que desinforma sobre algo, sino que impide creer en la verdad.

191 Aquí convendría plantearse si puede haber una hilo también con la legislación electoral.

192 “En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior” (artículo 86 LOPDDD).

motores de búsqueda¹⁹³, sino también a las redes sociales¹⁹⁴.

De igual forma que en el RGPD, la Ley que estamos comentado integra un derecho a la protección de los menores en Internet. Si bien el ordenamiento de la UE habla preferentemente de consentimiento, la legislación española va más allá y menciona una esfera más amplia en donde las obligaciones no sólo son para las empresas o los entes públicos, sino también para el propio entorno social. Claramente, esto tiene un carácter más bien inspirador y no tanto imperativo, puesto que habla del papel de los padres en el libre desarrollo de la personalidad¹⁹⁵. Para las empresas o instituciones que puedan vulnerar los

193 En concreto el artículo 93 ordena que “Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos...”.

194 Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

195 Específicamente, expone que “ Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales”.

derechos de un menor –sobre todo difundiendo informaciones o imágenes--, se establece la intervención del Ministerio Fiscal 2que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor”.

Además de estos derechos, la LOPDDD establece otros tantos que tienen que ver con el contexto laboral y que están a la orden del día, dadas las constantes polémicas sobre si una empresa tiene derecho a vigilar y controlar al trabajador en el espacio de trabajo y fuera de los horarios de oficina. Este debate se ha puesto de manifiesto en el actual contexto de pandemia por coronavirus que está afectando a millones de trabajadores en el mundo entero. Entre los derechos contemplados en este terreno por la LOPDDD, tenemos: el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (estableciendo unos límites para los empleadores con respecto a los empleados en el control del trabajo), el derecho a la desconexión digital en el ámbito laboral (para primar “el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar”) o los derechos digitales en la negociación colectiva (para que en los convenios colectivos haya

cláusulas que tengan por objeto proteger los derechos y libertades en torno a los datos personales.

Finalmente, otra novedad que introduce la norma española es la figura del derecho al testamento digital. Esto implica que los familiares de una persona fallecida puedan tomar control de las informaciones que ésta haya vertido en las redes sociales u otros medios y servicios de la Sociedad de la Información. Este derecho plantea una serie de cuestiones prácticas y de aplicabilidad.

Pero no sólo este derecho plantea esas cuestiones, sino quizá la totalidad de los que hemos enumerado aquí.

Por cuestiones de espacio no entraremos en el debate de la aplicabilidad real y práctica de los derechos digitales o en el de su papel como criterios inspiradores a la hora de la interpretación jurisprudencial (a la hora de emitir una resolución sobre un caso específico). Un sector de la doctrina considera que los derechos digitales son más bien unos derechos “etéreos”¹⁹⁶ que doctrinalmente hablando

196 En una conferencia reciente sobre derecho al olvido de la Asociación Peruana de Compliance, así se manifestaba el Letrado Leandro Núñez García, socio de la firma Audens Abogados de Nuevas Tecnologías. Sostenía que incluso pueden generar un conflicto de aplicación.

tienen un papel importante, pero que en la práctica aparecen en la Ley como redactados y salidos de un texto constitucional.

Lo anterior es así, porque el incumplimiento de esos derechos no acarrea sanciones ni ningún tipo de responsabilidad civil o penal, como si sucede en el caso de otros derechos fundamentales o con respecto a los propios principios de protección de datos.

Otro punto de vista es el del Ilustre Colegio de la Abogacía de Barcelona que ha diseñado y publicado una Carta por los Derechos de la Ciudadanía en la Era Digital con el fin de “garantizar que las mejoras indudables que los desarrollos tecnológicos aportan a la calidad de vida de las personas se lleven a cabo en el marco del respeto a los derechos humanos esenciales y los principios democráticos de las sociedades”. En esta Carta, por ejemplo, se agrega el “derecho a la identidad digital” y el derecho a la ciudadanía digital puesto que el individuo aparece “como sujeto que interactúa en los entornos digitales, generando relaciones jurídicas y obligaciones, especialmente en cuanto al uso responsable de las tecnologías de la información y comunicación”.

Por su parte, el Catedrático de Derecho Constitucional, Artemi Rallo Lombarte (quien fuera Director de la Agencia Española de Protección de Datos) se pronuncia más bien por una constitucionalización de los derechos digitales. Sobre esto, sostiene que “ resulta ineludible la necesidad de reconocer *nuevos derechos digitales* bien en el ámbito legal como constitucional (...). Una hipotética reforma de la Constitución debería incluir la actualización de la Constitución a la era digital y constitucionalizar una nueva generación de derechos digitales, de carácter sustantivo o prestacional” (Rallo, 2017: 666).

En conclusión, los derechos digitales reconocidos tanto en el Reglamento General de Protección de Datos de la Unión Europea como en la Ley de Protección de Datos y Derechos Digitales de España constituyen un avance relevante en la materia y sin duda, un antecedente legal y doctrinal necesario, de cara a su positivización a nivel constitucional y como criterios inspiradores para la jurisprudencia constitucional.

BIBLIOGRAFÍA

Arellano Toledo, W. (2019). “El derecho a la transparencia algorítmica en Big Data e Inteligencia Artificial”. *Revista General de Derecho Administrativo*, 50.

Arellano Toledo, W. (2017). “Privacidad e Internet de las Cosas”. *Revista de Derecho Digital*, 2-6: 25-56.

Guash Portas, V. (2012). “La transferencia internacional de datos de carácter personal”. *Revista de Derecho UNED* 11: 413-453.

Rallo Lombarte, A. (2017). “De la «libertad informática» a la constitucionalización de los nuevos derechos digitales (1978-2018)”. *UNED Revista de Derecho Político* 100: 639-669.

Normativa

Constitución Española, publicada en el *Boletín Oficial del Estado* de 6 de diciembre de 1978.

Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del Artículo 29, adoptado el 10 de abril de 2014.

Dictamen del SEPD sobre «Hacer frente a los desafíos que se plantean en relación con los macrodatos: llamamiento a la transparencia, el control por parte de los usuarios, la protección de datos desde el diseño y la rendición de cuentas».

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, publicada en el *Boletín Oficial del Estado* de 6 de diciembre de 2018.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), publicado en el *Diario Oficial de la Unión Europea* de 4 de mayo de 2016.

DOS SENTENCIAS INTERESANTES¹⁹⁷

Roberto Nelson Bugallo¹⁹⁸

RESUMEN:

La irrupción de las llamadas nuevas tecnologías fuerza a lxs actorxs jurídicos, y en especial a quienes se desempeñan en la docencia a revisar definiciones, sentencias y doctrinas que aún se encuentran en proceso de construcción. Por eso, cuando encontramos pronunciamientos judiciales que refieran al tema, prestamos especial atención a los posicionamientos de los partícipes y tratamos de compartirlos como material útil para la enseñanza del Derecho.

En dicho sentido, me pareció interesante referirme a dos sentencias recientes que involucran el uso de tecnologías digitales

PALABRAS CLAVE: *nuevas tecnologías, docencia, posicionamientos de los partícipes*

INJURIAS POR TWITTER

En marzo del corriente año, el Juzgado Correccional con sede en Olavarría, pero perteneciente al Departamento Judicial de Azul, dictó sentencia en una querrela iniciada por un docente de una escuela secundaria privada de esa localidad.

El mismo se habría sentido afectado por la publicación de unos twitters emitidos por un ex alumno de la institución, residente en La Plata, quien en ocasión de ver en un video las marchas a favor y en contra del proyecto de ley de despenalización del aborto, al detectar la presencia del Director en la concentración, escribió en Twitter: "XX, en

197 Enlace al video https://youtu.be/tM_a1YuAKCU

198 Docente investigador, Fac. de Cs. Jur. y Soc., UNLP; Fac. de Derecho, UBA; Fac. de Cs. Sociales, UNCPBA, integrante del GECSI -Grupo de Estudio de la Complejidad en la Sociedad de la Información- mail: robertobugallo@jursoc.unlp.edu.ar

marcha Provida en Olavarría. Cuando iba a la escuela (...) y él era director, un profesor acosó a una compañera nuestra. No sólo no lo echó, sino que nos dio una charla sobre cómo cuidarnos en las redes sociales, como si la piba tuviera la culpa. Hipócrita". "Mucha gente difundiendo este tweet. Aprovecho para decir que el profesor acosador era NN". El comentario fue recogido y viralizado por varias personas, incluida quien supuestamente fuera acosada que publicó también en Twitter "Esa piba soy yo. Hipócrita, que asco"

Tanto el Director como el docente aludido enviaron sendas cartas documento al ex alumno exigiendo retractación pública y una compensación económica bajo amenaza de accionar civil y penalmente, hasta finalmente el docente inició una querrela en los términos del art. 110 y 111 del Código Penal -injuria- que penaliza con multa de hasta veinte mil pesos dicha figura. Hasta aquí los hechos.

Sin embargo, en relación a uno de los ejes convocantes de este Encuentro, - Enseñanza e investigación en Derecho y Nuevas Tecnologías- creo que cabe deslizar algunas breves reflexiones.

A) Nuevas Figuras Productoras De Daño:

En primer lugar, las conductas reprimidas por los arts. 109 y 110 del C. Penal (calumnias e injurias) propaladas a través de las redes sociales o tecnologías digitales, cambian un escenario reservado a formas de comunicación mas tradicionales, (discursos, prensa escrita o medios de radiodifusión). Los rumores, críticas, comentarios, chismes u opiniones que anteriormente quedaban restringidos a circuitos mas o menos determinados, hoy se difunden a una velocidad asombrosa y sin encontrar límites previsibles a través de whatsapp, Instagram, Facebook, Tinder, Twitter o LinkedIn, u otra redes, y muchas veces permanecen allí alojados para quien quiera recrearlos, potenciando la memoria personal o colectiva.

El uso masivo de las redes sociales y las tecnologías digitales en las últimas décadas ha traído situaciones antes desconocidas obligando a articular otras respuestas desde el campo de lo jurídico, revelado muchas veces impotente o insuficiente frente al conflicto y que involucran el derecho a la comunicación, al honor, a la imagen o a la privacidad. Pornovenganza, (revenge porn), ciberbullying, stalking, sexting, grooming o

phishing, son algunas de las figuras incorporadas a los códigos penales o civiles ocasionadoras de daños, y cuya aplicación todavía está en proceso de elaboración jurisprudencial y doctrinaria.

B) Dificultades procesales:

Pero su instrumentación trae aparejadas algunas dificultades. Y uno de esos aspectos es el referido a la probanza. Las imágenes, posteos, mensajes o videos con potencialidad dañina que circulan por las redes sociales, muchas veces permanecen muy escaso tiempo circulando, por lo que es difícil utilizarlos como medio de prueba y para los operadores jurídicos se torna harto trabajoso brindar herramientas legales adecuadas. Las capturas de pantalla, sin certificación notarial, dentro de los procesos penales o civiles deben complementarse con otros medios de prueba como las respuestas de las compañías prestatarias de servicios de telefonía celular o de las proveedoras de internet, sumamente reacias a responder a oficios judiciales o extrajudiciales. Y a ello puede sumarse la utilización de perfiles falsos de usuarios

Sin embargo, hoy en día no es imposible para una nueva categoría integrada por

peritos informáticos o investigadores digitales descubrir e individualizar los teléfonos, computadoras, tablets, etc de donde provienen mensajes potencialmente dañinos.

En países europeos han surgido compañías o empresas especializadas en obtener una prueba digital, que actúan como “*terceros de confianza*” y que acreditan con un sello de tiempo, (*timestamp*) que un conjunto de datos existió en una fecha y hora concretas y que ninguno de estos datos ha sido modificado desde entonces. (ej. eGarante). Quizás no falte mucho para que alguna de esas empresas extienda actividades a estas regiones y apenas sea necesaria una modificación legal para validar la actividad.

C) Cuestiones de competencia:

La última reflexión (y puede haber muchas más derivadas de los conflictos que involucran a tecnología digitales y Derecho), refiere a un problema de competencia.

En el caso antes reseñado el imputado es alumno de la UNLP y se domicilia en la ciudad de La Plata. Los twitts fueron emitidos desde su teléfono celular. Se

planteaba la cuestión de competencia territorial: si era el lugar desde donde se emitieron los mensajes supuestamente lesivos o el lugar donde se habrían producido las consecuencias dañosas.

La jurisprudencia no es categórica. Uno de los pocos antecedentes refiere a calumnias e injurias vertidas en la ciudad de Bahía Blanca en comunicaciones epistolares dirigidas a la Dirección de Cultura y Educación y al Gobernador de la Provincia, ambos domiciliados en la ciudad de La Plata y fue resuelta a favor de la competencia del Juzgado Correccional Nro. 1 de Bahía Blanca (*"Incidente de competencia entre el Juzgado Correccional Nro. 1 –Bahía Blanca y el Juzgado Correccional Nro. 4 – La Plata" Causa Nro. 19759 Cámara de Casación Penal, Sala I, 25/08/2005*). Es de suponerse que al referirse al soporte digital utilizado, la jurisprudencia no alteraría la competencia territorial.

¿Y cómo termino la querrela? Con un veredicto absolutorio. El Juzgado entendió que el comentario involucraba un asunto de interés público por tratarse de un supuesto de violencia de género y estaba cubierto por la nueva redacción de las figuras de calumnias e injurias -Ley 26.551- sancionada por el Congreso de la Nación como resultado de la sentencia

emitida por Corte Interamericana de DDHH en el caso *Kimel Vs. Argentina*, -02/05/2008-.

N.N. c/FACEBOOK s/Habeas data

El otro caso judicial que encontré interesante refiere a una acción de habeas data –art 43 CN, 33 y cctes de la ley 25.326- presentada contra Facebook SRL en la justicia federal de La Plata por una persona que solicitaba se suprimieran ciertas URL con comentarios injuriantes en su contra, con una fotografía subida sin su autorización. Pedía se eliminaran dichos comentarios y datos subidos a la cuenta de la red INSTAGRAM. Solicitaba además información acerca de la identidad del titular de la cuenta, el correo vinculado, número de IP y otros datos a fin de instar una posterior acción por daños y perjuicios, afirmando que dichos comentarios lesionaban en forma continua y permanente sus derechos personalísimos al honor, la intimidad e imagen.

El reclamo se había originado por publicaciones difundidas a través de Facebook e Instagram en la cuenta denominada *"Comisión de Género"* existente en una de las Facultades de la

UNLP involucrándolo en presuntas conductas machistas, de abuso psicológico y manipulación vinculadas a una supuesta relación sentimental mantenida con una mujer anónima.

Señaló haber reportado en la plataforma de Facebook que dichas publicaciones resultaban lesivas a sus derechos y haber utilizado los recursos que sugiere la red para denunciar el comentario y los datos personales como perjudiciales, sin obtener respuesta, enviando posteriormente cartas documento a la dirección en la CABA de Facebook sin que fueran recibidas por la empresa.

Instada la acción, el Juzgado requirió el informe previsto por la ley 25.326 que fue respondido por la demandada y constató a través del Actuario la existencia de las publicaciones aludidas en la web. En la sentencia entendió que era de aplicación la doctrina de la CSJN sentada en *“Rodríguez María Belén c/Google Inc s/Daños y Perjuicios”* (28-10-2014) y que refería que a partir del momento de efectivo conocimiento por parte de la accionada del supuesto contenido ilícito de un página web, desaparece la “ajenidad” del buscador y se puede generar una responsabilidad por culpa al no bloquear dichos contenidos. Y concluye haciendo lugar a la acción de

habeas data contra Facebook SRL disponiendo que provea lo necesario para la eliminación de los URL e informe acerca del titular de las cuentas, el correo electrónico vinculado, número de IP, fecha, hora y eventualmente desde qué clase de dispositivo electrónico fueron subidos los comentarios y fotografía objeto de autos.

Esta sentencia fue recurrida por Facebook y resuelta por la Cámara Federal en junio del corriente año que la revocó y rechazó la demanda promovida, en un fundado dictamen del Dr. Vallefín al que adhirió el otro camarista.

En lo referente al eje convocantes de este Encuentro, -Enseñanza en Derecho y Nuevas Tecnologías- quiero destacar los siguientes puntos.

La accionada –Facebook- sostiene la falta de legitimación pasiva, indicando que el grupo Facebook instaló oficinas comerciales en la Rca. Argentina conformándose la sociedad Facebook Argentina S.R.L., cuyo objeto social es brindar soportes de venta para publicidad, marketing, relaciones públicas y comunicaciones, y cuya constitución fuera aprobada por la Inspección General de Justicia el 14/10/2011, diferenciándose de Facebook Inc, quien sí tendría

facultades para cumplir la manda judicial, pero que se domicilia fuera del país.

Tanto la sentencia de primera instancia como la de Cámara rechazan el planteo de falta de legitimación, acudiendo a jurisprudencia interna, refutando la desvinculación absoluta entre ambas sociedades comerciales, pero el voto de Cámara refiere especialmente a que las actividades vinculadas con la publicidad constituyen el medio para que la aplicación sea rentable y que esta estructura económica constituida por los recursos de los usuarios es la que permite el funcionamiento comercial de la empresa, debiendo por lo tanto regirse por la legislación local.

Ambas citan además precedentes del Tribunal de Justicia de la Unión Europea, (sentencia Lindqvist, C101/01, EU:C:2003:596 y COSTEJA y AEPD Vs. Google del 13 de mayo de 2014 (C131/12), rechazando la supuesta desvinculación entre las empresas locales y la central concluyendo que Facebook Argentina S.R.L. no puede eludir las mandas judiciales alegando que carece de facultades, por lo que debe cumplir con las resoluciones dictadas por los tribunales locales y notificadas al domicilio por ella constituido en el país.

El otro aspecto interesante de la sentencia de Cámara es el ámbito del discurso de la publicación difundida a través de la plataforma Facebook. Allí refiere a la especificidad de los motivos con que dicha publicación fue creada por la Comisión de Géneros de la Facultad de ...de la UNLP, “conformado por estudiantes autoconvocadxs desde julio de 2017, en el marco de una asamblea donde se mocionó la formación de ese espacio de mujeres e identidades disidentes”, constituyendo un foro de discusión, y un espacio de denuncia a políticas y prácticas, colectivas o individuales, consideradas lesivas a las perspectivas de género, y concluyendo que la publicación se hace cargo de un asunto de interés público que cuenta con protección constitucional y que impide su eliminación.

Un triple orden de razones abona esta afirmación: a) los sujetos que intervienen; -no son simples estudiantes, son militantes sociales de agrupaciones universitarias, con compromiso público-, b) el ámbito en que se discuten los hechos –una Facultad de una Universidad estatal- y c) el tema que involucra – comportamientos lesivos a las perspectivas de género-.

No es concluir que todas las publicaciones de Facebook estén revestidas del carácter de interés público, es que en este caso la articulación de los sujetos intervinientes, el ámbito de discusión y el tema convocante conforman áreas *“que preocupan, importan o interesan a toda la sociedad”* (“Fallos” 334:1722, considerando 14°, in re “Melo” con remisión a la Corte Suprema de los Estados Unidos en el caso ‘Gertz’, 418 US 323, 337), concluyendo *“que las manifestaciones de una agrupación que enarbola la defensa de las mujeres e identidades disidentes, denunciando que un militante se involucra en prácticas incompatibles con dichos ideales, debe considerarse un discurso amparado constitucionalmente”* Y frente a la situación de duda respecto de si un discurso en materia de género reviste carácter o no de interés público y si debe o no suprimirse, debe ser resuelta en favor de la protección constitucional de ese discurso y de su mantenimiento”. Y en consecuencia revoca la sentencia de primera instancia -11/06/2020-

En conclusión, sorprendentemente ambas sentencias además de involucrar a las tecnologías digitales -aplicaciones como Twitter y empresa Facebook- abordan

temáticas similares (*violencia de género*) y llegan a conclusiones parecidas (*discurso de interés público protegido*) y una y otra refieren al poder de viralizar la información con una extensión y rapidez desconocidas hace algunas décadas, confirmando un nuevo escenario cada vez mas específico en el tema pero a la vez mas extendido por su uso, en el que lxs distintos actorxs (judiciales o no) vamos aportando saberes, opiniones o reflexiones en una construcción colectiva en este relación entre el Derecho y las nuevas tecnologías

EL PASADO (¿QUE NOS PERSIGUE?) EN TIEMPOS DE INTERNET¹⁹⁹

Martina Andrea Gutiérrez Iuale²⁰⁰

RESUMEN

En la presente comunicación expondré la investigación realizada en el Taller de Seminario -materia del plan de estudios de la carrera de Abogacía (UNS)-, cuyo objetivo es enseñar a los estudiantes de grado a investigar, proponer hipótesis, refutarlas y/o comprobarlas a fin de introducirlo en la investigación científica.

La comunicación a desarrollar se centra en investigar el Derecho al olvido en Internet y la responsabilidad de los motores de búsqueda: analizando conceptualmente aquellos términos, los principales fallos jurisprudenciales, la evolución que ha tenido la temática en los últimos años y qué cambios -si los hay- pueden llegar a presentarse en el corto plazo.

Creemos que es un tema actual y de gran relevancia dada la afectación que puede llegar a tener un sujeto respecto de su identidad en las plataformas sociales del ciberespacio.

PALABRAS CLAVE: *derecho al olvido - internet - investigación - responsabilidad de intermediarios - motores de búsqueda - derechos personalísimos*

199 Enlace al video <https://youtu.be/KtZm2H9esBY>

200 Estudiante avanzada de la carrera de Abogacía de la Universidad Nacional del Sur. Mail: mgutierreziuale@gmail.com

INTRODUCCIÓN

La investigación desarrollada en el Taller de Seminario hizo foco en analizar la importancia de la protección de nuestros datos, imagen, honor e intimidad en internet; resolver lagunas generadas ante la falta de una legislación especial en la temática; delimitar cuestiones por las cuales debe ponderar el derecho al olvido en internet por sobre el derecho a la expresión e información, y comprender la importancia de su regulación y postura para futuros casos.

DERECHO AL OLVIDO EN INTERNET, ¿QUÉ ES?

El derecho al olvido en internet es el derecho que tiene toda persona de eliminar o solicitar que se elimine de los motores de búsqueda de internet información difamatoria sobre su persona, de su presente, o bien de su pasado que ya no se condice con su vida actual.

Este derecho está íntimamente relacionado con datos personales y el derecho a la intimidad, vida privada e íntima y derecho al honor.

Si bien los motores de búsqueda (tales como Google o Yahoo) no son los que producen la información, sí son los principales vehículos de la misma,

permitiendo que haya una difusión masiva sobre toda la comunidad cibernética. Estos buscadores indexan la información volcada a la web para que sea visible al momento de buscar información sobre la persona o tema en cuestión.

El derecho al olvido en internet comenzó a aplicarse desde 2014 en Europa y luego se extendió a otras latitudes. Desde esta comunicación se sostiene que es de gran importancia conocer su operatividad y aplicación, para preservar la intimidad de las personas que han sufrido una intromisión de su vida privada, o se ha menoscabado su persona mediante información falsa y tergiversada en su imagen u honor. También es menester tener en consideración, aquellos casos en donde las personas hubieran purgado una pena, y a pesar de ello su autoría en el hecho ilícito sigue apareciendo en los buscadores de internet.

Se pudieron encontrar posiciones encontradas tanto en el ámbito jurisprudencial como doctrinario. El debate en cuestión se ha centrado si la persona es funcionaria pública, si el tema era de interés público o no, la antigüedad de la información, si se trataba de una persona física o jurídica, y qué derechos se veían afectados.

Dentro de los autores que propician la ponderación del derecho a la intimidad, privacidad, honor, datos personales e imagen, por sobre el derecho a la información y expresión, Marcela Basterra (2014) expresa “...para que se configure la responsabilidad, se exige, por un lado, que el buscador tenga efectivo conocimiento de la ilicitud que un tercero efectúa respecto del nombre o imagen de una persona en una página web; y, por el otro, que pese a ello haya omitido eliminar el enlace en cuestión.”

En la misma posición Francisco Canese Mendez (2015) explica “...podemos concluir que cuando el derecho a la intimidad se ve afectado por el derecho a la libre expresión debemos analizar: a) en primer medida la existencia de interés público sobre lo informado y; en caso de inexistencia, b) si existieron factores eximentes que derriben la protección otorgada por el derecho a la intimidad a la información publicada (tales como la publicación voluntaria por parte del informado o el consentimiento otorgado por este en la publicación de la información). De no existir ninguno de estos casos, podremos concluir que el derecho a la libertad de expresión ES fue ejercido de manera abusiva, y el derecho a la privacidad sobre el de libertad de expresión”

En la vereda opuesta, autores como Molina Quiroga o Guillermo Peyrano sostienen la no aplicación del derecho al olvido, pues hacen hincapié en el descubrimiento de la verdad a través de la libre circulación de noticias, y que el derecho al honor no es absoluto sino que se encuentra limitado por los derechos fundamentales a opinar e informar libremente.

El fallo Belén Rodríguez.

En el año 2014 la Corte Suprema de Justicia de la Nación se expidió sobre la responsabilidad de los motores de búsqueda de internet, “Rodríguez, María Belén c/ Google Inc. s/daños y perjuicios” la actora había promovido una demanda por daños y perjuicios contra los buscadores Google Inc. y Yahoo de Argentina SRL.

La actora alegaba que se había procedido al uso comercial y no autorizado de su imagen y se habían avasallado sus derechos personalísimos al habérsela vinculado a determinadas páginas de Internet de contenido pornográfico. Además solicitó el cese del mencionado uso y la eliminación de todas las vinculaciones.

¿Eran los buscadores de internet responsables del uso de la imagen

indebida? La CSJN determinó una responsabilidad subjetiva por parte de Google y Yahoo. Si bien éstos no son creadores de contenido (sólo indexan la información obtenida según lo que el usuario busca), sí son pasibles de responsabilidad desde el momento en que toman conocimiento de dicha ilicitud (uso indebido de imagen, daño al honor...), aunque no atribuyó la misma responsabilidad en los denominados thumbnails.

Fallo Natalia Denegri

Recientemente, en agosto de 2020 la jurisprudencia fue más allá. La Sala H de la Cámara Nacional de Apelaciones en lo Civil confirmó la sentencia de primera instancia y aplicó el “derecho al olvido” por primera vez en la Argentina a favor de Natalia Denegri.

En autos “Denegri, Natalia Ruth C/ Google Inc S/ Derechos Personalísimos: Acciones Relacionadas” la actora solicitaba que se elimine información sobre ella de acontecimientos acaecidos hace más de 20 años y que la eliminación de dicha información no afectaría el interés público. En concreto el Tribunal ordenó a Google desindexar información de hace veinte años de la actora que nada tenía que ver con su vida actual.

En la sentencia se hizo mención del caso Mario Costeja en España en donde el actor solicitó eliminar datos suyos donde aparecía en un medio de comunicación de difusión nacional como deudor, fecha QUE databa de hacía más de 16 años; OBLIGANDO a Google a retirar de sus enlaces dicha información porque estos ya no eran pertinentes al tratarse de una información sobre una deuda comercial ya saldada que carecía de importancia en la actualidad.

Si bien en el fallo Denegri se menciona el antecedente español, El Tribunal lo diferenció del mismo ya que éste se relacionaba con una deuda impositiva en tanto que en el caso Denegri giraba en torno a una investigación penal, que luego fue cuestionada (“Caso Coppola”).

CUÁL ES LA IMPORTANCIA DEL FALLO DENEGRI

Por primera vez en Argentina se aplica el derecho al olvido en internet y obliga a la empresa Google a desindexar y eliminar enlaces que relacionaban a Natalia Denegri con hechos acaecidos hace más de veinte años.

A diferencia del fallo Belén Rodríguez, donde se la relacionaba a la modelo con sitios pornográficos y la responsabilidad

de los buscadores de internet, afectando el honor de la persona, en Denegri pudo determinarse que los hechos acontecidos eran de larga data, y carecían de interés público y por lo tanto eran pasibles de ser eliminados.

Además esta sentencia a mi entender de ningún modo configura una censura a la libertad de expresión ya que los enlaces que conducían a las noticias carecían de carácter informativo trascendental para la sociedad sobre algo sucedido en los años '90.

CONCLUSIONES

Sin dudas el derecho al olvido en internet es un tema de gran actualidad y que si bien ha sido receptado por la Sala H de la Cámara Nacional en lo Civil, no hay decisiones finales al respecto, ya que Google ya habría apelado la sentencia ante la Corte Suprema de Justicia de la Nación, y también conforme evoluciona la tecnología y las herramientas que utilizan los motores de búsqueda para indexar contenido en la web se presentan cada vez nuevas situaciones.

Nuestro país aún no cuenta con una regulación legislativa sobre la responsabilidad de los motores de búsqueda en Internet, en relación con el

contenido generado por terceros. En el Congreso de la Nación si bien hubo un proyecto de ley sobre la temática, el mismo perdió recientemente estado parlamentario.

Es menester que deba analizarse cada caso para establecer si es factible aplicar el derecho al olvido en internet, teniendo en cuenta algunas cuestiones básicas como: relevancia pública del caso (por ejemplo, no es lo mismo un acto de corrupción que es de interés público judicial y socialmente, con un persona que ya purgó su pena por una causa penal pero ese hecho sigue apareciendo en los motores de búsqueda al averiguar en internet sobre esa persona. Pensemos por ejemplo en alguien que atropelló y mató a un peatón, cumplió su pena en tiempo y forma, pero los sitios webs siguen mostrando aquel accidente, generando un menoscabo en la persona que ya cumplió con la pena impuesta por la justicia penal.

Asimismo, fallo Denegri, abre una puerta de por más interesante para intercambiar ideas y opiniones sobre el derecho al olvido en internet, qué responsabilidad tienen los motores de búsqueda en estos casos y en qué casos debería aplicarse, ya que la línea entre el derecho a la información y los derechos personalísimos aún es muy delgada.

BIBLIOGRAFÍA CONSULTADA:

- BASTERRA, Marcela, I. “La responsabilidad de los motores de búsqueda de Internet en el centro del debate jurídico”, LA LEY 05/11/2014, 05/11/2014, 1 - LA LEY2014-F, 145, (LaLey Online p. 6).

- CANESE MENDEZ, Francisco. “Medidas cautelares e Internet. Libertad de expresión y privacidad”. LA LEY 06/04/2015, 06/04/2015, 5, (AR/DOC/976/2015, p. 5)

MOLINA QUIROGA, Eduardo, “Rechazo a una medida cautelar innovativa contra la red social Facebook”, SJA 2014/06/18-12 ; JA 2014-II, (ABELED0 PERROT N°: AP/DOC/876/2014, pp. 10-11). y - PEYRANO, Guillermo F. “Nuevas problemáticas del tratamiento de datos personales. El tratamiento de informaciones que proporcionan datos personales por parte de medios periodísticos a través de internet”, SJA 7/4/2004 ; JA 2004-II-1217, (ABELED0 PERROT N°: 0003/010468, pp. 8, 11, y 15).

- LEZCANO, José María, “Análisis de la Responsabilidad Civil de los Buscadores de Internet”, Anales de la Facultad de Ciencias Jurídicas y Sociales; año 7, no. 40, 2010. p. 530.

Jurisprudencia consultada:

Caso "Rodríguez, Maria Belén c/ Google Inc. s/ daños y perjuicios".

Caso “Denegri, Natalia Ruth C/ Google Inc S/ Derechos Personalísimos: Acciones Relacionadas” (Sala H de la Cámara Civil).

RESPONSABILIDAD CIVIL DE LAS PLATAFORMAS DIGITALES FRENTE AL CONSUMIDOR²⁰¹

Florencia Romina Gianfelici^{202*}

RESUMEN

El comercio electrónico ha experimentado un crecimiento exponencial en los últimos tiempos. Este incremento en el volumen de operaciones consolida una tendencia que se viene gestando desde antaño. Por ende, lo novedoso no es el medio empleado sino la velocidad con que se posicionó como el modo de contratación por excelencia.

En este contexto, en la doctrina y en la jurisprudencia se discute cuál es la responsabilidad de las plataformas digitales, que proporcionan el espacio de intermediación donde se concretan dichas operaciones, frente a eventuales daños sufridos por los consumidores electrónicos.

Del análisis de los fallos propuestos resulta que no es del todo conveniente trasvasar automáticamente soluciones propias de otros derechos, sin hacer las adecuaciones que nuestro ordenamiento exige, al extremo de llegar a atribuir “propia torpeza”, a quien simplemente se confió en la seguridad que la plataforma de comercialización le inspiraba.

Palabras clave: comercio electrónico; plataformas digitales; consumidor; responsabilidad civil; daño.

201 Enlace al video <https://youtu.be/mMEnIn27XWY>

202* Abogada egresada de la Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional del Litoral. florenciarominagianfelici@gmail.com

INTRODUCCIÓN

El comercio electrónico ha experimentado un crecimiento exponencial en los últimos tiempos. Así, la Cámara Argentina de Comercio Electrónico (CACE) afirma que en el mes de Abril se registró un 84% más de facturación que el promedio de ventas del primer trimestre del año en curso (Cámara Argentina de Comercio Electrónico [CACE], 2020).

Este incremento en el volumen de operaciones consolida una tendencia que se viene gestando desde antaño. Por ende, lo novedoso no es el medio empleado sino la velocidad con que se posicionó como el modo de contratación por excelencia.

En este contexto, en la doctrina y en la jurisprudencia se discute cuál es la responsabilidad de las plataformas digitales, que proporcionan el espacio de intermediación donde se concretan dichas operaciones, frente a eventuales daños sufridos por los consumidores electrónicos.

Es por ello que a fin de indagar en esta cuestión analizaremos dos fallos que resolvieron en sentidos contradictorios el tema bajo estudio.

LOS CASOS EN ANÁLISIS

El fallo “Kosten”. (Kosten, Esteban c/ Mercado Libre SRL, 2018)²⁰³

Esteban Kosten, compró un automóvil a través del conocido sitio web, Mercado Libre. Tras intercambiar reiterados mails con un supuesto vendedor, efectuó una transferencia internacional para pagar el precio fijado y así concretar la operación. Pero la entrega del vehículo nunca se efectivizó. Por tal razón interpuso acción de daños y perjuicios contra Mercado Libre SRL, invocando su carácter de proveedor de la cadena de comercialización conforme al art. 40 Ley 24.240.

La sentencia de primera instancia admitió la excepción de falta de legitimación pasiva interpuesta por el demandado. La Cámara confirmó tal decisorio conforme los argumentos que enuncio a continuación.

Se sostuvo que siendo que en el ordenamiento jurídico argentino no existe normativa regulatoria de la situación de referencia, resulta de vital importancia las soluciones que existen en el Derecho comparado como parámetro para resolver el *thema decidendum*.

203 En igual sentido, Besler, Darío c/ Mercado Libre SRL (2019).

Se invoca en este orden la Directiva 2000/31/CE del Parlamento Europeo y del Consejo que, al analizar aspectos vinculados a la sociedad de la información, establece reglas relativas a la responsabilidad de los prestadores de servicios informáticos. La misma distingue dos tipos de supuestos según cuál sea la participación de las plataformas digitales en el intercambio de bienes y servicios. En tal orden, los prestadores podrían tener una posición neutral en el intercambio si se limitan a un mero tratamiento automático y técnico de los datos suministrados por sus clientes; o un rol activo si además de ello, se presta asistencia a los usuarios a fin de optimizar o promover las ofertas formuladas por los proveedores.

La distinción es importante pues sólo en el primer supuesto, los prestadores no estarían obligados a supervisar o controlar los datos que se almacenan dentro de sus servidores. Tampoco tendrían el deber de realizar búsquedas activas sobre hechos ilícitos que podrían derivar de los mismos, pero de tener conocimiento de ellos, la Directiva les impone el deber de comunicarlos con la mayor prontitud posible a las autoridades públicas competentes.

De manera tal, que cabrá al órgano jurisdiccional analizar en cada caso cuál

ha sido el rol del administrador del mercado electrónico en el marco de intercambio de bienes y servicios.

En concordancia con esto, la Cámara sostuvo que Mercado Libre resistió la pretensión del actor aludiendo que dicha plataforma de ventas o subastas *on line* opera desde dos secciones, a saber: a) Sección de *marketplace*, destinada a la compraventa de bienes no registrables, en la que los datos de los vendedores son dados a conocer una vez que las ofertas son aceptadas; y b) Sección clasificados, abocada al intercambio de bienes registrables, en donde aquellos datos están publicados con la misma oferta.

El decisorio adujo que la plataforma de referencia tuvo una posición neutral, constituyendo un “mero canal” al haberse vinculado el actor y el vendedor del automotor por fuera de la misma y de manera totalmente independiente a ella. Advirtió que el prestador que gestiona el mercado electrónico no desempeña una función de corredor, es decir no se obliga frente a las partes a la conclusión de determinados negocios. Sino que se limita a proporcionar un foro de transacción que pone en contacto a las partes.

Descarta el tribunal que resulte de aplicación el art. 40 de la Ley 24.240, el que sólo sería aplicable en aquellos casos

en que, involucrado un consumidor, se pruebe la participación activa del administrador del mercado electrónico en la operatoria.

Consideran así de aplicación lo dispuesto por la CSJN respecto de los motores de búsqueda (Rodríguez, María Belén, c/ Google Inc., 2014, considerando 16), sosteniendo que a la inexistencia de la obligación general de vigilar le sigue, como regla, la inexistencia de responsabilidad. En este orden, sostienen que se verifica en el caso bajo análisis un supuesto de responsabilidad subjetiva. De manera tal que para pretender acreditar la responsabilidad de dicho operador económico, el actor debería acreditar la “ignorancia premeditada” o la “indiferencia imprudente” de dicho agente que no resultaría responsable por el carácter ilícito del contenido en sí, sino por su omisión o actitud negligente (inadecuada, incompleta o tardía) en retirar los contenidos o en bloquear su acceso.

Por último, se sostuvo que el actor fue víctima de su propia torpeza (Art. 1111 Cod. Civ. y 1729 CCCN) en tanto que no tomó los recaudos que debería haber adoptado quien adquiere un automotor, e hizo caso omiso a las advertencias de Mercado Libre, entre otras, la de usar su propia plataforma de pago y no una alternativa.

El fallo “Mercado Libre”. (Mercado Libre SRL c/ Dirección de Defensa del Consumidor y Lealtad, 2020).

El 17 de Octubre de 2014 la Dirección General de Defensa del Consumidor y Lealtad Comercial de la Provincia de Córdoba impuso una multa de \$20.000 a la firma Mercado Libre por considerar que infringió la Ley de Defensa del Consumidor (arts. 4, 9, 11, 13 y 34). La denuncia que motivo tal decisión fue interpuesta por la señora Carolina Nilda Grifasi al no encontrar respuesta por parte de dicho sitio web frente a los reclamos que había formulado con motivo de recibir unas zapatillas usadas y correspondiente a una marca distinta a la que había comprado como nuevas.

Tras diversas vicisitudes procesales, la cuestión llegó al Tribunal Superior de Justicia de la Provincia de Córdoba a fin de revisar la sanción administrativa impuesta.

Si bien el fallo en análisis, no surge de una demanda judicial contra Mercado Libre, como en el caso analizado en el apartado precedente, resulta interesante su estudio porque se discurren, en sentido contrario, los argumentos analizados previamente.

De más está decir, que el actor fundamentó su pretensión invocando su carácter neutral, es decir, alegó que no tiene ningún tipo de vinculación con los productos que se comercializan por ese medio informático. Sostuvo que sólo es un proveedor de los servicios que ofrece y publicita a través de Internet pero no es distribuidora de los bienes que se comercializan por esa vía. Razón por la cual entendió que no debe considerársela inmersa dentro del art. 40 de la ley 24.240. Que una decisión en ese sentido haría inviable la actividad que desarrolla generando la oportunidad para que un sin número de demandas se alcen en su contra. Ello sin contar el efecto perjudicial que se extendería a todo el entramado social como consecuencia de la desaparición de este modo de contratación.

Por otra parte aludió a que tampoco sería pasible de responsabilidad en razón de conexidad contractual, en tanto que la misma no se verifica en el caso de marras. Los contratos celebrados por dicha empresa con cada uno de las partes de la operatoria, como los perfeccionados entre estas entre sí, son contratos independientes sin una finalidad económica común a ellos, que justifique la aplicación de esta figura.

Frente a los argumentos esgrimidos por Mercado Libre, el Tribunal enunció las consideraciones que menciono a continuación.

Sostuvo el tribunal que en relación a la conexidad contractual, la misma se verifica toda vez que el ingreso al sistema por el vendedor y el comprador se realiza con la finalidad de concretar una operación de intercambio. Es decir, ninguno de ellos accede al premencionado sitio web sin ninguna razón, por lo contrario, lo hace para comprar o para vender algo. De manera tal que los contratos, que habilitan el uso de la plataforma, léase aceptación de términos y condiciones, tienen en mira esta intención de las partes, y a su vez dichos negocios encuentran razón de ser en las posteriores operaciones que se celebren.

Aclara el tribunal que esta conclusión resulta más patente aún si se entiende que Mercado Libre asume el carácter de “proveedor de servicios” al ofrecer de manera profesional un ámbito virtual, para que quienes demanden y ofrezcan bienes se contacten, celebren y perfeccionen acuerdos con dichos fines. Este rol activo en el perfeccionamiento de los contratos luce cada vez más evidente si se toma en cuenta las prestaciones adicionales que dicha plataforma ha ido incorporando para

generar confianza en los consumidores y fomentar la utilización del sitio web. Tales la calificación de usuarios, plataformas de pago, sistemas de envíos propios, mecanismos de solución de controversias, entre otros.

Se sostuvo que esa confianza, sumado al beneficio económico que Mercado Libre puede obtener de manera directa o indirecta de tales operatorias, justifica la aplicación de las normativas del derecho del consumo. Más aún si se piensa que la parte compradora reviste el carácter de consumidor en los términos del art. 1 de Ley de Defensa del Consumidor.

Tal es la consideración de Mercado Libre como miembro de la cadena de comercialización, que el Tribunal consideró que la sancionada incumplió con el deber de información a su cargo. Si bien es cierto que no podría obligársela a controlar la totalidad de los productos ofertados a través de su plataforma, si le sería posible exigir a los proveedores que allí publicitan un detalle minucioso de los productos ofertados. De suerte tal que si tomara conocimiento de alguna irregularidad, debería darla a conocer a sus usuarios, conjuntamente con los medios legales propicios para hacer frente a cualquier perjuicio que podrían sufrir.

EL DIÁLOGO

Como hemos visto, ambos fallos coinciden en que la comercialización a través de plataformas digitales, como Mercado Libre, es una actividad compleja²⁰⁴, con particularidades que deben ser analizadas caso por caso, pero sin que ello sea óbice para aplicar reglas generales imperantes en la materia.

La tecnología profundiza más aún la vulnerabilidad de los consumidores, que lejos de aprovechar las ventajas que ofrece Internet resultan perjudicados si no saben manejarlo o lo hacen deficientemente. En este contexto, el deber de información se intensifica, no solo por lo extraño y dificultoso del medio empleado, sino por el hecho de que la decisión de compra se realiza en función de los datos suministrados por el proveedor al no poder el consumidor tener contacto directo con el producto.

La cuestión pasa por delimitar el ámbito de responsabilidad de las plataformas digitales dentro de las operaciones realizadas a través de Internet (Gianfelici y Gianfelici, 2020).

204 Al punto tal que en el primer fallo analizado se difiere respecto de la regulación de honorarios en primera instancia por considerar que la ausencia de un marco normativo específico podría haber generado dudas respecto al derecho del actor en reclamar.

Si bien es cierto que no contamos en nuestro derecho interno con normas específicas que regulen la responsabilidad de los proveedores de este tipo de plataformas²⁰⁵, el Anteproyecto del Código de Defensa del Consumidor (ACDC) la consagra expresamente. Así el Art. 73 sostiene: *“Portales de venta o subasta on line. De conformidad con las reglas de conexidad, la exención de responsabilidad del operador electrónico sólo será posible cuando se configure alguno de estos extremos: 1) No ha desempeñado un rol activo en la operación jurídica-económica, limitándose a proporcionar únicamente un foro de transacciones, informando ello de forma clara, destacada y fácilmente comprensible; 2) No ha generado una particular confianza en el consumidor”*.

Se despeja con este artículo las discusión que mencionamos *ut supra* sobre la existencia de conexidad contractual en este tipo de operatorias, al remitirse expresamente a aquella normativa. Se consagra a su vez como regla la responsabilidad de las plataformas digitales previendo dos eximentes (Cancio, 2019).

205 Ello sin perjuicio de algunas normativas de naturaleza internacional que se han mencionado en Estevarena y Barocelli (2018).

Parece útil el criterio mencionado en el primero inciso que busca distinguir aquellos supuestos donde tales plataformas tienen un rol activo en la contratación, de aquellos otros en lo que su posición es neutral. Ya hemos visto, conforme a lo sostenido en el fallo “Kosten”, que nos ubicamos en uno u otro caso según que podemos afirmar que Mercado Libre tiene o no conocimiento y control de los datos almacenados por sus usuarios, independientemente si cobra por la prestación del servicio (Barry y Bauer, 2018). Ahora bien, no resulta tan claro cuándo se verifica en la práctica tal situación.

Considero que afirmar que Mercado Libre es un mero proveedor del software de la plataforma de intermediación y no de los productos en sí, no es razón suficiente para liberarlo de todo tipo de responsabilidad. Semejante afirmación conduciría indefectiblemente a admitir la existencia de un proveedor que puede actuar en el mercado sin ningún tipo de riesgos a costa de la desprotección de los consumidores.

Claramente, Mercado Libre no es un mero foro de transacción, sino que facilita el contacto y acerca a las partes. Los usuarios ingresan a dicha plataforma en virtud de la confianza que dicha empresa les merece. Tal confianza, la rapidez con

las que se concretar las operaciones, la accesibilidad a las ofertas y la rigurosa especialidad del servicio prestado, debe ser algo especialmente ponderado a la hora de analizar su responsabilidad (Tambussi, 2018).

Por ende, más allá de la vaguedad del término confianza, al que alude la segunda eximente, debe analizarse esa particular apariencia que el proveedor genera en el consumidor (Trivisonno, 2018), que lo determina a elegir esa plataforma y no otra. Más aún si Mercado Libre -como se menciona en el segundo fallo analizado-, “destaca su rol económico y social como agente generador de puestos de trabajo, oportunidades de negocios, igualdad y democratización del comercio tanto en Argentina como en Latinoamérica”.

Sostener que los casos de marras constituyen supuestos de responsabilidad subjetiva, implicaría afectar severamente el sistema protectorio del consumidor, obligándolo a producir pruebas diabólicas que no está en condiciones de procurar. De lo contrario deberíamos concebir el estándar de un consumidor medio, como lo hace el Derecho comparado, con cierto nivel de instrucción y de información, despierto y diligente, cuya vulnerabilidad deba ser analizada caso por caso (Estevarena y Barocelli, 2018). Esta idea

desnaturaliza nuestro concepto nacional de consumidor. De ahí que la eximente del hecho de la víctima en materia de consumo es de interpretación restrictiva y sólo procede ante la prueba de una culpa grave o dolo del damnificado (Conf. art. 115 ACDC) (Sozzo, 2017).

CONCLUSIÓN

Por ello, considero que no es del todo conveniente trasvasar automáticamente soluciones propias de otros derechos, sin hacer las adecuaciones que nuestro ordenamiento exige, al extremo de llegar a atribuir “propia torpeza”, a quien simplemente se confió en la seguridad que la plataforma de comercialización le inspiraba.

La organización de un sistema digital de comercialización, conlleva beneficios económicos, pero también riesgos, lo cual es un todo indivisible. Las plataformas digitales no pueden pretender disfrutar de los primeros y soslayar los últimos.

REFERENCIAS

- Cámara Argentina de Comercio Electrónico. (26 de Mayo de 2020). *El comercio electrónico creció 84% en abril*. <https://www.cace.org.ar/noticias-el->

[comercio-electronico-crecio-84-en-abril#:~:text=El%20comercio%20electr%C3%B3nico%20en%20Argentina,un%2071%25%20en%20unidades%20vendidas.](#)

- Kosten, Esteban c/ Mercado Libre SRL s/ ordinario; Cámara Nacional de Apelaciones en lo Comercial, (sala D). (22 de Marzo del 2018). Recuperado de la base de datos Información Legal Online La Ley, AR/JUR/1780/2018.

- Besler, Darío c/ Mercado Libre SRL s/ Sumarísimo. Cámara de Apelaciones de Comodoro Rivadavia, (sala B). (27 de Mayo de 2019). Recuperado de la base de datos Información Legal Online La Ley, AR/JUR/28824/2019.

- Rodríguez, María Belén, c/ Google Inc. s/ daños y perjuicios. Corte Suprema de Justicia de la Nación. (28 de Octubre de 2014). Recuperado de la base de datos Información Legal Online La Ley, AR/JUR/50173/2014.

- Mercado Libre SRL c/ Dirección de Defensa del Consumidor y Lealtad Comercial s/ recurso de apelación c/ decisiones de persona jurídica pública no estatal – recurso directo. Tribunal Superior de Justicia de la Provincia de Córdoba, sala civil y comercial. (19 de Mayo de 2020). Recuperado de la base

de datos Información Legal Online La Ley, AR/JUR/16523/2020.

- Estevarena, E. y Barocelli, S., (2018). La protección de los consumidores en plataformas de comercio electrónico. *Diario La Ley*, 30 de Febrero de 2018; p.6. Recuperado de la base de datos Información Legal Online La Ley, AR/DOC/870/2018.

- Gianfelici, M. y Gianfelici, F., (2020). Legitimación pasiva del consumidor frente a la responsabilidad civil por actividades riesgosas o peligrosas. *Revista de la Facultad de Ciencias Jurídicas y Sociales. Balance a cinco años de vigencia del Código Civil y Comercial de la Nación (2015-2020)*, Nueva Época, nº 11; p.183-192.

<https://bibliotecavirtual.unl.edu.ar/publicaciones/index.php/NuevaEpoca/article/view/9595/12858>

- Cancio, S. J., (2019). Comercio electrónico: la posición neutral de la plataforma y la negligencia del consumidor como eximentes de responsabilidad. *La Ley Patagonia*, 23 de diciembre de 2019, p. 3. Recuperado de la base de datos Información Legal Online La Ley, AR/DOC/3755/2019.

- Barry, L. D. y Bauer, E., (2018). El rol activo como dirimente en materia de responsabilidad en el comercio

electrónico. *Diario La Ley*, 2 de Febrero de 2018, p. 6. Recuperado de la base de datos Información Legal Online La Ley, AR/DOC/825/2018.

- Tambussi, C. E., (2018). Relación de consumo y responsabilidad objetiva entre los usuarios de plataformas de venta y el proveedor del servicio. *Diario La Ley*; 22 de Mayo de 2018. Recuperado de la base de datos Información Legal Online La Ley, AR/DOC/789/2018.

- Trivisonno, J. B. (2018). Comercio electrónico, responsabilidad y confianza. *SJA*, 17 de Octubre de 2018. Recuperado de la base de datos Información Legal Online La Ley, AR/DOC/3455/2018.

- Sozzo, G., (2017). La responsabilidad de los proveedores de juegos mecánicos"; Sección de Jurisprudencia obligaciones. *Revista de Derecho Privado y Comunitario Nº 2017-3*, Rubinzal-Culzoni, p. 411-445.

NÓMADAS DIGITALES²⁰⁶

Verónica S. Arizcuren²⁰⁷

RESUMEN:

La Revolución 4.0, también conocida como Cuarta Revolución Industrial, moviliza al mundo laboral tradicional. Cambió el eje del trabajador que va a su lugar de empleo, en días de semana y horarios fijos bajo las ordenes de un solo empleador. Ahora el trabajo es el que va a la persona. El Nómada Digital es aquel que se conecta mediante el uso de las TICS, de manera remota desde cualquier parte del mundo, permitiéndole trabajar por objetivos bajo sus propios horarios. Es un proceso socioeconómico y laboral del Siglo XXI en fase inicial que implica la liberación del profesional respecto a barreras geográficas, se rompen las estructuras laborales tradicionales produciendo su flexibilización. El objetivo de esta investigación es describir que es un Nómada Digital, tipos, cuáles son sus motivaciones y los desafíos que implica para los países establecer un marco regulatorio de esta nueva modalidad laboral, siendo clave la negociación colectiva.

PALABRAS CLAVES: Nómada digital – Revolución 4.0 – Trabajo Remoto – TICS– Flexibilización

206 Enlace al video <https://youtu.be/DEyAjiFILM>

207 Abogada, egresada de la Universidad Nacional del Sur. Mail: veroarizcuren@gmail.com

INTRODUCCIÓN: LA REVOLUCIÓN 4.0

A lo largo de la historia de la humanidad, hemos atravesado la transformación y evolución del trabajo humano a través de cuatro procesos históricos conocidos como “Revoluciones Industriales”. El primero se trató del paso de la producción manual a la mecanizada entre 1760 y 1830. En el segundo se introdujo la electricidad, lo que permitió la producción en masa. Con la llegada de la electrónica y las Tecnologías de la Información y la Comunicación (en adelante TICS) a mediados del Siglo XX, fue la Tercer Revolución Industrial. Actualmente, nos encontramos atravesando la Cuarta Revolución, conocida como “Revolución 4.0”, hay una automatización de los procesos con los sistemas ciberfísicos, se combina maquinaria física con digitalización, que transforma el producto final²⁰⁸. En una publicación reciente, Gilda Fiatti y Mónica Carrizo postulan que: *“La cuarta revolución industrial se revelará con mayor impacto a partir de los avances en la internet de las cosas, el análisis de*

208 Wulf, Erico, *“El valor del trabajo en la revolución industrial 4.0. Desafíos para la gestión de personas y competitividad”* Publicado en Revista de Derecho laboral y Seguridad social, Thomson Reuters La Ley, mayo 2020. Cita online: AR/DOC/4028/2019.

*macrodatos, la computación en la nube y la inteligencia artificial. La internet de las cosas conectará no solo a personas, sino también a objetos dotados de capacidades de detección, procesamiento y comunicación de información digital. Esta infraestructura generalizada iniciará una colosal cantidad de datos, que podrá utilizar para acrecentar la eficiencia en términos de producción y distribución de bienes y servicios.”*²⁰⁹

En el marco de una crisis energética e importantes congestiones en el tránsito, surgió en Estados Unidos, la idea del teletrabajo, estableciéndose leyes que obligaban a las empresas a efectuar proyectos de teletrabajo con el fin de reducir el tráfico y la contaminación ambiental y a mediados de la década del ´80, los países europeos comienzan a implementar esta nueva modalidad laboral en sus empresas. Miguel Ángel De Virgiliis y Martín Ignacio De Virgiliis lo definen como: *“El fenómeno que consiste en la realización de todo trabajo por parte de personal vinculado con la entidad destinataria del mismo, sin la presencia física del trabajador en esta última, utilizando a tales efectos métodos de*

209 Fiatti, Gilda y Carrizo, Mónica, *“El valor del trabajo en la cuarta revolución industrial: las plataformas digitales”* Publicado en Revista de Derecho laboral y Seguridad social, Thomson Reuters La Ley, junio 2020. Cita online: AR/DOC/4035/2019.

procesamiento electrónico de información –tecnologías de la información y la comunicación, TIC- y manteniéndose contacto entre las partes a través de la utilización regular de medios de comunicación idóneos que generan un valor agregado.”²¹⁰

La figura del teletrabajo comenzó a ser utilizada mundialmente por las empresas y los organismos públicos, asimismo surgieron subtipos como los Trabajadores Nómades Digitales.

¿QUÉ ES EL TRABAJO NÓMADA DIGITAL?

Se trata de un proceso socioeconómico y laboral que surge en el Siglo XXI, que implica la liberalización del trabajador respecto a barreras geográficas, rutinas y horarios fijos, hay una ruptura de las estructuras laborales tradicionales, cuyas herramientas principales son las TICS, aplicaciones de software y el trabajo en la nube. Son personas que viajan por el mundo, lo que les permite combinar trabajo y vida personal, conocer nuevos lugares y nutrirse de distintas

210 De Virgiliis, M. A. y De Virgiliis, M. I., “*El teletrabajo. La nueva realidad virtual*” (2003), Revista de Derecho Laboral, Rubinzal Culzoni Editores, pag.346.

experiencias laborales, lo que hace un trabajador enriquecido en sus conocimientos, suele teletrabaja en *coworking*, cafés, *home office* o librerías.

Es un estilo de vida elegido por profesionales itinerantes de entre 20 y 35 años de edad, relacionados en su mayoría con el entorno digital: marketing, comunicación, diseño gráfico y programación web suelen ser las ocupaciones más frecuentes. Sin embargo, hay trabajadores remotos que ejercen como agentes comerciales o de atención al cliente e, incluso, como psicólogos a distancia, que han logrado darle una vuelta a su profesión para poder realizarla desde cualquier lugar del mundo. Esto implica que se trata de personas altamente capacitadas, tanto en su preparación específica respecto al trabajo que desarrollan como en el manejo de la tecnología y el conocimiento de distintos idiomas. Para los empresarios, este sistema les permite contratar a empleados sumamente capacitados, sin importar en qué lugar del mundo se encuentren, sin tener gastos de traslados o mudanzas innecesarias. Precisamente lo describe la Dra. Viviana Díaz, en su libro “Teletrabajo y neurotecnología, Una guía imprescindible para gestionar el trabajo 4.0”: “*Flexibilidad y agilidad son características que*

demandan los trabajadores del conocimiento, y así surge una nueva modalidad del trabajo: el Trabajador Conectado Remotamente como un sistema de gestión integrado que busca mejorar la calidad de vida de las personas que trabajan en una organización, hacer más eficientes los espacios, reducir tiempos y gastos de traslados.”²¹¹

TIPOS DE TRABAJADORES

Relación de dependencia: hay trabajo subordinado, la prestación de la actividad es efectuada por el trabajador por cuenta ajena bajo la dirección y el mando de otra persona, mediante el uso de elementos informáticos. Existen dos formas de impartir órdenes desde el empleador al dependiente: 1) Trabajador conectado *on line* con la empresa: esta imparte mandatos de trabajo y controla la ejecución del mismo en forma instantánea, aquí la tecnología facilita la vigilancia y supervisión. 2) Trabajador *off line*: no hay conexión directa con la empresa, el teletrabajador está desconectado del computador central, recibe instrucciones iniciales y remite el

211 DIAZ, Viviana, “Teletrabajo y neurotecnología, Una guía imprescindible para gestionar el trabajo 4.0” (2018). Ediciones Granica S.A., pag.149.

resultado de su labor, lo que se conoce como Trabajo por objetivos.

Autónomo: son los casos en que se encomienda a una persona la realización de una obra determinada, quien la lleva a cabo, asume los riesgos y utiliza sus propias herramientas de trabajo.

LEGISLACIÓN APLICABLE. LA NEGOCIACIÓN COLECTIVA

Recientemente, en el marco de la pandemia por el COVID-19, fue dictada en nuestro país la Ley N°27555 que regula el Régimen legal del Teletrabajo, la cual comenzará a regir recién a los 90 días de finalizado el Aislamiento social, preventivo y obligatorio. La misma ha sido objeto de varias críticas por el sector empresario, sin embargo me enfocaré en destacar artículos como: la reglamentación del Derecho a la desconexión digital (art.3), la compensación de gastos (art.10) y en especial el Art. 17 que menciona el caso de que existan Prestaciones Transnacionales: “Cuando se trate de prestaciones transnacionales de teletrabajo, se aplicará al contrato de trabajo respectivo la ley del lugar de ejecución de las tareas o la ley del domicilio del empleador, según sea más

*favorable para la persona que trabaja. En caso de contratación de personas extranjeras no residentes en el país, se requerirá la autorización previa de la autoridad de aplicación. Los convenios colectivos, acorde a la realidad de cada actividad deberán establecer un tope máximo para estas contrataciones.*²¹²

dicho artículo es aplicable a los trabajadores nómades digitales y si bien merece algunas críticas, considero que es un buen punto de partida a nivel nacional.

En el ámbito internacional, la Organización Internacional del Trabajo (OIT) en el año 1996 dictó el Convenio sobre el trabajo a domicilio, el mismo fue ratificado por nuestro país por la Ley 25.800. Se trata de una norma suprallegal que contempla en sus disposiciones todo tipo de trabajo a distancia entre los que se encuentra el teletrabajo. Asimismo, en el año 2002, la Confederación Europea de Sindicatos (CES), la Unión de Confederaciones de la Industria y de Empresarios de Europa (UNICE), la Unión Europea del Artesanato y de la Pequeña y Mediana Empresa (UNICE/UEAPME) y el Centro Europeo de la Empresa Pública (CEEP) firmaron un acuerdo marco sobre

el teletrabajo a fines de dar seguridad a los teletrabajadores por cuenta ajena en la Unión Europea, el cual se configura como un marco general de ámbito europeo que establece disposiciones mínimas y básicas sobre las que debe ser la regulación del Teletrabajo en cada uno de los Estados miembros.

La multinacional *Telefónica*, llevó a cabo una prueba piloto con el objetivo de identificar las actividades susceptibles de ser desarrolladas por teletrabajadores, el Convenio Colectivo de Telefónica de Telecomunicaciones tomó los principios recogidos en el Acuerdo Marco Europeo y suscribieron un acuerdo con los empleados donde detallaron las condiciones, con principios como el de voluntariedad y reversibilidad como rectores.

En Argentina, uno de los convenios más innovadores fue el de la Federación de Sindicatos Unidos Petrolíferos e Hidrocarburíferos (SUPEH) suscripto en el año 2014 donde regularon la operación de sistemas de telesupervisión, coordinación de yacimientos, automatización de plantas, entre otras actividades, el cual tenía un periodo de vigencia de 36 meses; en el 2017 presentaron la reforma de este Convenio Colectivo de Trabajo, introduciendo definitivamente el Trabajo

212

<https://www.boletinoficial.gob.ar/de talleAviso/primera/233626/2020081>

4

Remoto como modalidad. No fue menos la Federación Argentina de las Telecomunicaciones (FATEL), que en el 2011 lo reguló en su CCT junto a la Federación de Obreros y Empleados de Telecomunicaciones (FOETRA).

Concluyendo, la evolución del derecho es más lenta que la de las TICS y las nuevas formas de trabajar que surgen en el mercado, hay un evidente atraso en la legislación y en las negociaciones colectivas. Se critica a los sindicatos por no amoldarse a nuevos tipos de contrataciones, cuyas gestiones continúan desarrollándose como lo hacían 50 años atrás, teniendo como modelo la relación de empleo tradicional. La cuestión radica en que se deberían aunar criterios de acción los gobiernos, las organizaciones empresariales y los sindicatos, en donde el eje sea el trabajador contemporáneo que enfrenta los desafíos de un mundo globalizado y en crecimiento permanente.

BIBLIOGRAFÍA

De Virgiliis, M. A. y De Virgiliis, M. I., *“El teletrabajo. La nueva realidad virtual”* (2003), Revista de Derecho Laboral, Rubinzal Culzoni Editores, pag.346

Diaz, Viviana, *“Teletrabajo y neurotecnología, Una guía imprescindible para gestionar el trabajo 4.0”* (2018). Ediciones Granica S.A., pag.149.

Fiatti, Gilda y Carrizo, Mónica, *“El valor del trabajo en la cuarta revolución industrial: las plataformas digitales”* Publicado en Revista de Derecho laboral y Seguridad social, Thomson Reuters La Ley, junio 2020. Cita online: AR/DOC/4035/2019.

Wulf, Erico, *“El valor del trabajo en la revolución industrial 4.0. Desafíos para la gestión de personas y competitividad”* Publicado en Revista de Derecho laboral y Seguridad social, Thomson Reuters La Ley, Mayo 2020. Cita online: AR/DOC/4028/2019.

IMPRESIÓN 3D INTELIGENTE Y DESEMPLEO CON SUS RESPECTIVAS CONSECUENCIAS EN EL DERECHO²¹³

Manuel Martín Pino Estrada²¹⁴

RESUMEN:

La impresión 3D es una forma de imprimir cosas de todo tipo directamente de la computadora, tablet o celular, pudiendo recibir prototipos por la internet, sea email, whatsapp, telegram u otra forma de comunicación, pero cuando se junta con la inteligencia artificial, ésta permite una impresión muy precisa del objeto conforme el comportamiento del material utilizado, haciendo que la mano de obra humana sea dejada de lado en muchas áreas de la Economía, pues la impresión 3D inteligente permite que cualquier persona, física o jurídica fabrique cosas en su lugar de origen, desde juguetes, armas, prótesis, ropas, piezas de carro hasta casas, puentes y edificios sin necesidad de trabajadores, provocando desempleo y consecuencias también en los derechos de autor y en la producción de pruebas.

Palabras claves: *Impresoras - Derecho - Trabajo – Industria*

213 Enlace al video https://youtu.be/0mjBa1_r88I

214 Magister en Derecho en la Universidad Federal do Rio Grande do Sul (UFRGS). Profesor de la Escuela Superior de Abogacía de la Orden de los Abogados de Brasil – Sección São Paulo – capital/Brasil. Email: martinpino@yahoo.com

INTRODUCCIÓN

La presente comunicación trata sobre los impactos de la impresión 3D en las diversas áreas de la Economía y del Derecho, provocando grandes consecuencias laborales y legales, más aún cuando se junta con la inteligencia artificial, como es en el caso del Derecho de autor, Derecho del Trabajo, Derecho Civil, Penal y también en las cuestiones de pruebas materiales, pues esta tecnología ya permite imprimir en tres dimensiones las pruebas mostradas en las fotos cuando acontecen crímenes, por ejemplo, de allí viene la importancia de su estudio en el Derecho y es lo que se pretende demostrar en las líneas que se siguen

LA IMPRESIÓN 3D

La impresión 3D no está siendo una revolución en bits sino en átomos, aparte de ser una fabricación doméstica, la impresión 3D sería la invención más revolucionaria desde el invento de la imprenta de Gutenberg 600 años atrás. La impresora 3D usa un archivo digital escaneado que es enviado para ella misma por una computadora o similar. La impresión es hecha con un plástico líquido gota a gota o utilizando un láser para fundir materiales como metales y otros

más duros, de esta forma un archivo de un prototipo puede convertirse en un objeto listo para usarlo y sin necesidad de importarlo de algún país o comprarlo en la tienda de la esquina si se puede conseguirlo dentro de la casa, lo que pasa es que ésto ya está provocando desempleo en varias áreas de la Economía, más aún cuando se junta con la inteligencia artificial.

El sistema de impresión 3D examina minuciosamente cada capa del objeto mientras se imprime, ella mismo corrige los errores en tiempo real. Esta información es utilizada por el sistema de aprendizaje automático para predecir el comportamiento de la deformación de los materiales y de esta forma tener los productos finales con mayor precisión. Para garantizar la calidad, la máquina conserva una réplica digital. Con esta tecnología, la impresora 3D puede imprimir materiales más flexibles (que suelen ser más difíciles de imprimir) y con geometría compleja con mayor precisión. Por ejemplo, imprimir un chip de computadora, que es una pieza llena de detalles minuciosos, siendo así mucho más precisa.

Nada de ésto, sin embargo, funcionaría tan bien sin la unión de la impresora 3D con la inteligencia artificial que le dice a la

propia impresora qué hacer, de esta manera el margen de error se reduce significativamente al entrenar el algoritmo del software de la impresora. Cada parte nueva trae mejoras debido al algoritmo de aprendizaje de la máquina, que hace que corrija sus errores, así el resultado es la producción de piezas con alta definición. Esto es fundamental para la fabricación automatizada de cohetes, satélites, varios dispositivos y piezas en otros planetas debido a la carrera espacial existente, por que para imprimir cosas en Marte se necesita de un sistema adaptable a condiciones muy inciertas, y por eso se está desarrollando una estructura de algoritmos inteligentes que se puedan transferir para líneas de producción a ser instaladas en otros mundos utilizando la vía sistema de comunicación entre la Tierra y los planetas que se pretenden visitar.

IMPRESIÓN 3D Y DESEMPLEO

La unión de la impresión 3D con la inteligencia artificial va a provocar desempleo en muchas áreas, como las que se siguen:

a). médica: imprimiendo prótesis dentales, de brazos, piernas, cráneos, piel humana hasta órganos humanos (bioimpresión 3D);

b) industria textil: ropas hechas en casa a la medida de la persona sin necesidad de irse a una tienda de ropa;

c) industria de calzados: zapatos, zapatillas, botas etc a la medida de la persona hechas en casa;

d) industria de carros y afines: piezas de carros, ómnibus y tractores;

e) industria espacial: piezas para cohetes y piezas para usarlas en la Luna y en otros planetas;

f) industria armamentista: hacer revólveres, ametralladoras y hasta balas (algo polémico);

g) industria de juguetes: cada uno podrá hacer el juguete a su gusto para sus hijos y para los amigos adultos;

h) industria de computadores; piezas de laptop, tablets etc.

i) alimentación: impresoras 3D que hacen comida, como chocolates, tortas (de matrimonio, o de cumpleaños, por ejemplo), dulces y hasta panes;

j) construcción civil: casas, edificios, puentes y afines;

k) de muebles: imprimir sillas, sofás, mesas y material de oficina;

l) industria musical: imprimir instrumentos musicales como tambores, teclados hasta guitarras;

m) industria naval: barcos y cruceros;

n) industria de la robótica: impresión de robots en gran escala.

La impresión en 3D está demostrando que al entrar en estas áreas laborales va a provocar el despido de muchos profesionales que irán al desempleo, pues junto con la inteligencia artificial que corrige los errores automáticamente junto con el comportamiento del material en el momento de la hechura de la cosa que se quiere imprimir va a ser muy difícil competir, a parte de que va a haber menos intermediarios, disminuyendo los gastos para las empresas en ir a las fábricas de repuestos, por ejemplo, haciendo que el producto final sea más barato y de mejor calidad conforme el material usado.

Cuando se refiere a un producto más barato, se puede entender que cada vez más se podrá importar menos productos manufacturados de la India, China y de otros países con legislaciones laborales mínimas, inclusive favoreciendo la desaparición del trabajo esclavo, como por ejemplo en el área de la costura, pues una impresora 3D tiene condiciones de

reemplazar muchos costureros al hacer ropas, lo mismo en el área de piezas electrónicas de celulares, de carros y de barcos incluyendo las áreas ya mencionadas anteriormente.

LA IMPRESIÓN 3D EN OTRAS ÁREAS DEL DERECHO

impresión 3D en algunas áreas del Derecho.

En la cuestión de pruebas

Es posible en cuestiones que se necesiten pruebas materiales, como son los casos de un revólver que fué arrojado en un río para que no lo encuentren, pero al ver la foto o video se lo puede imprimir en una impresora 3D, lo mismo se puede hacer con cuchillos y otros tipo de prueba material en las áreas civil y laboral, como cosas diversas y documentos escritos, inclusive, se puede imprimir en 3D el escenario de un accidente o tiroteo junto con los cuerpos, por ejemplo.

En los derechos de autor

Desgraciadamente la jurisprudencia en Brasil no acompañó lo avances tecnológicos. La Ley nº 9.610, de 1998 que rige los derechos autorales en Brasil

está desactualizada, eso se entiende por que en la época de su creación no se imaginó que se podría llegar tan lejos. El artículo 7º de la ley dice: “Son obras intelectuales protegidas las creaciones del espíritu, expresadas por cualquier medio ou fijadas en cualquier soporte, tangible o intangible, conocido o que se invente en el futuro”, eso no está claro para los días de hoy.

El Marco Civil de la Internet, Ley nº 12.965, de 2014 no especifica sobre descargas por internet de objetos ya patentados, pues no es sólo imprimir en 3D algo que está en la internet y todo está resuelto, por esta razón es deber de las empresas y de los usuarios conseguir informaciones sobre quien hizo la obra disponible en la internet, si tiene derechos autorales o si tiene un código de software abierto, caso contrario, quien imprime sin seguir estas recomendaciones podrá ser enjuiciado y sufrir las consecuencias legales.

Justamente, para evitar consecuencias legales ya existen páginas web especializadas en la divulgación de archivos que son permitidos por los mismos autores para que sus inventos sean reproducidos o perfeccionados, inclusive, hay autores que permiten la reproducción de sus inventos si el uso no

es comercial, hay otros que no dan ninguna restricción y por último, existen otros autores que sólo permiten su impresión con cobranza de derechos autorales.

CONCLUSIONES

La impresión 3D va a provocar más desempleo aún pues se juntó con la inteligencia artificial al permitir la fabricación en pequeña, media y gran escala de productos que antes uno que tenía que ir a una tienda o importar de un otro país para conseguirlo, esta situación ya está pasando en toda la industria y en servicios básicos como de una panadería hasta ropas, todo pudiendo ser hecho en casa y listo para su uso respectivo, hasta los intermediarios de estos productos tendrán que buscar outra forma de renta pues ya están desapareciendo.

La solución está en políticas públicas de mejoría de la educación, educando desde niños a que ellos crien e inventen cosas útiles y tengan contacto con la robótica e informática, pues el hecho de dejar a los hijos con un celular el día entero produciendo datos y así trabajando gratis para las empresas de tecnología no es la solución. En las facultades de Derecho aquí en Brasil deben enseñar a los alumnos lenguajes de programación y

Derecho Digital, algo que el mercado ya está exigiendo.

REFERENCIAS

Brasil. Ley de Derechos Autorales. Disponible en:

http://www.planalto.gov.br/ccivil_03/leis/l9610.htm Acceso en 20 set. 2020

Brasil. Marco Civil de la Internet. Disponible en:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acceso en 22 set. 2020.

O futuro da impressão 3D – Paulo Farias, Stratasys. Disponible en:

<https://www.youtube.com/watch?v=Vk3weOHcHDw> Acceso en 25 set. 2020.

Print the legend. Disponible en:

<https://www.netflix.com/br/title/80005444> Acceso en 20 set. 2020.

RETOS DE LA REGULACIÓN ESTATAL DE LA DESINFORMACIÓN EN EL CIBERESPACIO E INTERNET²¹⁵

Ernesto Ángeles Guerrero²¹⁶

RESUMEN:

El fenómeno de la desinformación es un fenómeno complejo que ha crecido en los últimos años gracias a la aparición y consolidación de diferentes tecnologías relacionadas al ciberespacio y su funcionamiento y, mientras existen diferentes perspectivas de cómo regular el problema, siempre subyace la pregunta ¿Qué áreas son efectivas de regular?. La desinformación es un problema cibernético y de comunicación, por tanto, no es suficiente regular o censurar los mensajes, sino atender el proceso completo.

PALABRAS CLAVE: *Desinformación, ciberespacio, internet, perspectivas regulativas, regulación estatal*

215 Enlace al video <https://youtu.be/p5MZhBGoRck>

216 Maestro en relaciones internacionales por la Universidad Nacional Autónoma de México, investigador y presentador en el programa InfodemiaMX del Sistema Público de Radiodifusión del Estado Mexicano (SPR).
Correo: ernesto.angeles.a12@gmail.com

INTRODUCCIÓN

Los beneficios que el ciberespacio y sus tecnologías asociadas brindan a la comunicación en la sociedad no son unidireccionales, algunos generan y significan riesgos, vulnerabilidades y peligros, los cuales se materializan por medio de los emisores, receptores, mensajes, canales y contextos tecnológicos relacionados en el entorno de la información de cada país.

Uno de estos problemas es la sobreabundancia de información y el uso malicioso de ésta para llevar a cabo campañas, operaciones o actividades de desinformación con el fin de satisfacer objetivos particulares, aún así estos sean en contra del interés, la salud o la seguridad pública, ciudadana o nacional.

El intentar regular desde el Estado el problema de la desinformación conlleva una serie de cuestiones a tener en cuenta: ¿se debe regular el contenido?, ¿el canal?, ¿los emisores?, ¿o tal vez la estructura tecnológica (y con ello el internet y el ciberespacio)? ¿Cuál es el papel de los receptores de información y qué acciones podrían llevar a cabo? Entre muchas otras.

El objetivo que persigo en esta discusión es analizar la complejidad que significa

para el Estado crear diferentes mecanismos de regulación con el fin de disminuir el fenómeno de la desinformación, así como identificar áreas generales de falencia y limitaciones en los diferentes paradigmas regulatorios que tienen como opción los Estados.

La desinformación implica información falsa o manipulada que es compartida con la intención de causar daño y puede entenderse como un subconjunto de la propaganda²¹⁷. Pertenece a lo que algunos autores denominan como “Wicked problems”²¹⁸.

Debido a diferentes eventos locales, nacionales e internacionales²¹⁹, el combate contra la desinformación se ha posicionado como un tema importante en la agenda internacional y de los diferentes gobiernos, entre estos enfoques destacan: Regulación vertical

217Montgomery, M. (2020). Disinformation As a Wicked Problem: Why We Need Co-Regulatory Frameworks. Foreign Policy at Brookings, (August), 1–14

218 Son inestables, socialmente complejos y difíciles de definir claramente; tienen múltiples interdependencias y múltiples causas; no tienen una solución clara y crean consecuencias imprevistas cuando se intentan solucionar; involucran el cambio de comportamiento y la acción de muchos actores diferentes dentro y fuera del gobierno; y dejan a su paso una serie de intentos fallidos de políticas para resolverlos.

219 De entre estos resalta fuertemente el impacto internacional de la intromisión rusa en las elecciones presidenciales estadounidenses en 2016, el cual significó un cambio de paradigma en la lucha y atención del problema de desinformación en el ciberespacio e internet

tradicional²²⁰; -Auto regulación de actores relevantes²²¹ -Regulación multistakeholder²²²

ELEMENTOS DE LA DESINFORMACIÓN Y LAS OPCIONES REGULATIVAS DEL ESTADO

Paradigma regulativo	Datos personales y publicidad	Contenido	Herramientas	Transparencia	Algoritmos y estructuras digitales
Tradicional					
Auto-regulación					
Multistakeholder					

El Estado se enfrenta a que la mayoría de entidades con grandes capacidades en internet son principalmente de Estados Unidos o China, lo que significa que el tratamiento, almacenamiento y exploración de datos personales están sujetos a marcos normativos externos y, en muchos de los casos, sujetos también a locaciones físicas extraterritoriales, aunque esto no es excluyente con las

²²⁰ Este modelo se caracteriza por dotar al Estado y sus instituciones de capacidades regulativas suficientes de manera vertical y centralizada

²²¹ La auto regulación apela a la capacidad de las redes sociales y otros actores importantes dentro del ciberespacio e internet para establecer estándares y buenas prácticas acorde a sus compromisos, capacidades e intereses.

²²² El enfoque multistakeholder apela a la capacidad de cooperación y coordinación de todos los actores interesados bajo la coordinación de actores relevantes como el Estado.

leyes de protección de datos personales de cada Estado, aunque sí les resta efectividad.

Además del problema de la locación de datos está el modelo económico de publicidad, plataformas, servicios digitales y terceras partes, del cual es posible regular y minimizar sus riesgos y peligros, aunque no modificar sustancialmente ya que este problema está relacionado al diseño y funcionamiento de la tecnología, lo que implica directamente el equilibrio de poder del sistema internacional y el papel que los Estados y sus actores relevantes tienen en el ciberespacio e internet²²³.

La regulación del contenido es un tema muy complejo, en la regulación vertical los Estados autoritarios tienen ventaja por sobre los países democráticos debido a las pocas restricciones y respeto de los derechos humanos, y aún dentro de los países democráticos hay discrepancias en cuanto a la regulación del contenido²²⁴.

²²³ La nacionalidad de los servicios y estructura de internet y el ciberespacio viene de la mano de intereses, valores y objetivos de cada país y el caso del "libre tránsito de la información" es un claro ejemplo de las prioridades e hibridación entre tecnología y política exterior, dado que el tema es una piedra angular en la política exterior estadounidense y cualquier cambio sustancial a este modelo tendría que asumir los costos políticos que esto significa, sobre todo si la dependencia internacional hacia EUA es fuerte.

²²⁴ Mientras que Estados Unidos propone un modelo de libertad casi total en el ciberespacio e internet, la Unión Europea es más prohibitiva a la hora de regular su espacio digital.

Debido a la versatilidad del ciberespacio e internet, los contenidos son muy variados, por lo que se requeriría establecer un sistema de vigilancia, cooperación con empresas, censura en línea y, en general herramientas de regulación que hagan posible que el Estado pueda bloquear o censurar el contenido en línea, aunque esto se antoja difícil aún para países como China o Rusia.

La autoregulación del contenido de los actores del ciberespacio genera suspicacias a la hora de pensar ¿Quién y cómo se determinaría la censura de contenido, bajo qué parámetros?, ¿Es viable que un actor privado regule actividades que bien podrían considerarse como parte del debate público?

La regulación del paradigma multistakeholder propone una serie de elementos, pesos y contrapesos institucionales y de poder entre las partes; sin embargo, esta propuesta tiene como supuesto la participación amplia de actores de la comunicación que, según el contexto, algunos son parte del problema de la desinformación, por tanto, regular el contenido sería, en el mejor de los casos, dañar sus intereses o simularlo.

En la autorregulación de empresas como Facebook y Google, el tema de la transparencia, los intereses comerciales,

así como los derechos de propiedad intelectual se presentan como retos considerables a atender bajo un modelo económico de extractivismo de datos, lo que significa que su impacto de acción está íntimamente relacionado en cómo esto afecta su modelo de negocio.

Por último, el enfoque más conveniente a estos problemas el del multistakeholder, en el cual se invita a todos los interesados en torno a un conflicto a encontrar soluciones comunes; sin embargo, esta suposición se da entre una serie de presupuestos que escapan mucho de realidades en países como los latinoamericanos, donde los conflictos de intereses y correlación de capacidades son muy desiguales.

En el caso del diseño y funcionamiento algorítmico de la tecnología y los servicios digitales resalta la potestad de los actores con mayores capacidades y, sobre todo, con la titularidad de la propiedad intelectual, lo que significa que cualquier intento de regulación de parte del Estado tiene que adecuarse a la negativa de acceso a ciertos elementos tecnológicos, lo que hace de la auto regulación y regulación multistakeholder la mejor opción.

Además del funcionamiento y diseño estructural de internet y el ciberespacio,

resaltan otros elementos del problema de la desinformación que son necesarios transparentar para así poder regular o atender más puntualmente, tal como los datos sobre campañas de desinformación o nombres y donatarios en publicidad o campañas digitales.

Mientras que el modelo de la auto regulación y multistakeholder se adapta más en la prevención y mitigación del problema, el modelo de regulación jerárquico se adapta en la disminución de los problemas antes que en la prevención, ninguno es la solución definitiva, sino que cada uno atiende situaciones distintas de acuerdo a sus capacidades de poder.

Regulatory Frameworks. Foreign Policy at Brookings, (August), 1–14.

BIBLIOGRAFÍA CITADA

- Montgomery, M. (2020). Disinformation As a Wicked Problem : Why We Need Co-