

9o. CONGRESO IBEROAMERICANO DE INVESTIGADORES Y DOCENTES DE DERECHO E INFORMÁTICA (RED CIDDI)

Resumen de Conferencias y Trabajos

Aída Noblia

Introducción

El 9o. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (Red CIDDI) tuvo lugar del 9 al 11 de mayo de 2019 en la Sede Central de la Asociación de Escribanos del Uruguay (AEU), Montevideo, Uruguay, organizado por la Comisión de Derecho Informático y tecnológico) (Comisión DIT) del Instituto de Investigación y Técnicas Notariales (IITN).

La Red CIDDI es una Red Académica de Universidades e Instituciones de Investigación y Enseñanza dirigida a un conocimiento no solo teórico sino que también posibilite y estimule el desarrollo de aplicaciones prácticas que mejoren la calidad de vida de las personas de cada entorno.

El **Eje temático** seleccionado por quien suscribe para el Noveno CIDDI fue **“Informática, Ética y Derecho”** entendiendo que además de los aspectos técnico informáticos y jurídicos, los éticos son esenciales para que el proceso de cambio de época que vivimos redunde en beneficio de la humanidad.

El tratamiento de los temas propuestos se desarrolló en siete **Bloques Temáticos**: I. Gobierno Digital, derecho a la verdad, desafíos. II Derechos humanos, protección de datos personales. III Ciberdelitos. Avances en la investigación. IV. Comercio Electrónico, protección del consumidor electrónico. Nuevos modelos de negocios. VI Documentación, notarios, registros públicos y nuevas tecnologías. VII Acceso a la información pública, justicia abierta, informática forense. En dichos Bloques se expusieron Conferencias y Trabajos escritos. Estos últimos fueron previamente presentados, sometidos a revisión y los aprobados por el Comité de Honor fueron expuestos presencialmente por sus autores en el Evento. A continuación realizamos un resumen de las Conferencias expuestas en el Evento. Los trabajos se pueden visualizar íntegros en el sitio en Internet del Congreso.

Conferencia inaugural y Videoconferencias

La **Conferencia Inaugural** sobre **“La revolución digital en las telecomunicaciones: una visión de su impacto en la sociedad”**, a cargo del Ingeniero Industrial Electrónico Juan Piaggio, docente de Ingeniería Telemática en la Universidad de Montevideo, Uruguay, asesor de Vicepresidencia de la Administración Nacional de Telecomunicaciones (ANTEL), Uruguay. El Ingeniero enfocó los aspectos técnicos que ameritan la calificación

de revolución a este cambio de la tecnología analógica a la digital y sus diferentes etapas y generaciones de estas tecnologías (1G a 5G) que usamos a diario en celulares y diferentes tipos de aparatos, definidas por la Unión Internacional de Telecomunicaciones (UIT o ITU por sus siglas en inglés). Reflexionó sobre el impacto que han sufrido las generaciones de personas que vivencian el acelerado cambio, mas que las que desde que nacieron casi se encuentran con estos aparatos.

Se exhibieron dos **Videoconferencias**: una sobre **“La regulación de los territorios inteligentes. Un boceto cartográfico de las fuentes de la Unión Europea”** del Profesor Manuel D. Masseno, docente e investigador del Instituto Politécnico Beja Lab de Lisboa, Portugal, del Instituto Brasileiro de Direito da Informática (IBDI) en Brasil. Expuso sobre territorios Inteligentes, desde un punto de vista global, viendo al territorio como unidad física, ya sea ciudades, áreas protegidas, territorios rurales, territorios turísticos, en su interacción con las nuevas tecnologías aplicadas a ellos.

Este enfoque global que se da por una visión económica de aprovechamiento de recursos, si bien genera su optimización y resultados positivos, mediante racionalización de dichos recursos, por otro lado es un riesgo a tener en cuenta y controlar, respecto a derechos fundamentales como la privacidad entre otros y es posible base del “capitalismo de vigilancia”, “sociedad del control” y de vigilancia masiva.

El hipercontrol mediante redes de sensores hiperconectados, uso de grandes cantidades de datos (big data, datos masivos, comunicación en banda ancha, aprendizaje automatizado, etc) atenta contra un orden jurídico que intenta controlarlo, en Europa a través de Directivas y Reglamentos sobre seguridad de los sistemas de redes, control de acceso a datos y protección de datos personales, en diversos países mediante diferentes herramientas, incluida la privacidad por diseño y la aplicación de principios en el uso de los datos, tales como limitación al uso exclusivamente para la finalidad para la que fueron recabados, entre otros.

La otra Videoconferencia titulada **“Internet como Derecho Humano”** de Romina Florencia Cabrera, Abogada y docente argentina, complementa y reafirma la anterior en relación al destaque de los Derechos Humanos y recalca la preocupación por cumplir la finalidad de protección de los referidos derechos en el ámbito de Internet.

Se expusieron y discutieron además, diez conferencias y catorce trabajos presentados y aceptados luego de su revisión.

Conferencias

En el **Bloque II** relativo a **Derechos Humanos y Protección de datos personales**, el Abogado español Luis López Loma, especialista en Derecho asociado a las nuevas tecnologías y Director de Leynet Consultores con sede en España expuso sobre **“El Reglamento europeo de Protección de Datos y su aplicación extraterritorial”** de interés académico y práctico a nivel mundial, ya que la protección otorgada por el Reglamento (RGPD) se aplica a personas físicas, independientemente de su nacionalidad

o lugar de residencia, respecto al tratamiento de sus datos personales. Dicho tratamiento debe estar concebido para servir a la humanidad. Establece principios a respetar por empresas y quienes colectan datos personales. (deben colectarse de manera lícita, leal y transparente, usarse solo para la finalidad para la que fueron colectados, deben ser exactos, adecuados, pertinentes actualizados, razonables, entre otras características. El responsable del tratamiento de datos, establecido dentro o fuera de la Unión Europea, debe cumplir el RGPD. El derecho a la protección de los datos personales no es absoluto: debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. Se aplica no solo en territorio europeo sino a los datos personales de individuos europeos que se encuentren en cualquier parte del mundo, y a personas de cualquier nacionalidad que se encuentren en territorio europeo; también a la transferencia de datos desde la Unión a otros países, restringiéndola en los países que carezcan de un nivel adecuado de protección de datos personales, de acuerdo al RGPD, dado que la mayoría de los países aún carecen de dicho nivel. La alineación a las normas del RGPD, que se exige a los países con los que se negocia o trata, es un control importante; no es fácil de cumplir para el resto de los países. Pero su cumplimiento trae ventajas:: evita sanciones, reduce riesgos de ataques cibernéticos, mejora reputación, aumenta confianza de clientes y control de flujo de información y ayuda a no perder mercado de UE a las empresas que lo cumplen. No regula: tratamiento de datos personales de personas jurídicas y empresas constituidas como personas jurídicas, incluido: nombre, forma de la persona jurídica y sus datos de contacto.

En el **Bloque IV** sobre “**Inteligencia Artificial y Robótica**” la conferencia “**Inteligencia artificial. Derechos y Responsabilidades**” de María José Viega Abogada, Escribana y Docente del Centro de Derecho Informático de la Facultad de Derecho de la Universidad de la República, Uruguay, continuó la línea de defensa de los Derechos Humanos y principios éticos en el ámbito específico de la inteligencia artificial (IA), mencionó los siete principios establecidos por Google entre los que destacamos: fomentar IA socialmente beneficiosa, evitar sesgo injusto, seguridad, responsabilidad, privacidad por diseño, mantener altos estándares científicos y estar disponible para usos acordes a dichos principios. Mencionó los principios y estrategia de AGESIC (que es la Agencia del Gobierno uruguayo que gestiona lo relativo a sociedad de información y conocimiento), la necesidad de proteger derechos humanos respecto a IA. Como desafíos tecnológicos para los seres humanos señaló el peligro de concentración del poder en una minoría poseedora de las fuentes de información y datos frente a una mayoría que se torna insignificante, pérdida de trabajos, de libertad debido al uso de macrodatos enfocados a personas y de igualdad, en tanto quienes poseen datos podrán manejar al resto de las personas. Desde el punto de vista jurídico los derechos de propiedad intelectual son desafiada por la producción de las máquinas, la ciberseguridad es un desafío constante a la vez que una herramienta, según quien use las IA, problemas éticos en tanto el robot puede tomar decisiones dañinas para la vida humana, en ciertos casos no previstos, por ejemplo de vehículos autónomos u otras máquinas o aparatos. Respecto a responsabilidades jurídicas de las conductas exigidas por la ley a los sujetos responsables se aplicará según los casos la responsabilidad civil contractual o extracontractual, la responsabilidad penal por dolo o culpa solo sería aplicable a personas físicas, la del

Estado podrá exigirse por falta de servicio y en el mercado de consumo se podrá exigir responsabilidad al proveedor por productos o servicios que no cumplan los requerimientos legales o técnicos u ocasionen daños al consumidor.

En el mismo Bloque el Abogado Hugo Álvarez Saez, fundador del Programa Nacional de Ciencia y Justicia (CONICET), integrante del Cuerpo de Investigaciones Judiciales, Coordinador del Laboratorio de Innovación e Inteligencia Artificial de Universidad de Buenos Aires, expuso el tema **“La cultura infinita. El Derecho, la Ética y la Inteligencia Artificial predictiva”**: En el abordaje del ambiente perijurídico donde se cruzan informática, técnica y justicia se sugieren reflexiones sobre la inteligencia artificial, una ‘constelación’ de procesos y tecnologías. Se dice que las máquinas pueden funcionar según los mismos conceptos y reglas que la inteligencia humana. No es así. Generalmente optimiza la ejecución de tareas computarizadas, asignadas por seres humanos. Las profundas mutaciones que producen las innovaciones técnicas predictivas suelen tener lados luminosos y oscuros. Habrá que mirar la nueva realidad desde el ser Antrobiológico en que nos venimos transformando entre el ser biológico y el robótico, a fuerza de prótesis, chips, sensores, decisores, redes neuronales que nos proyectan a un infinito dirigido por quienes manejen los algoritmos. Es necesaria una regulación gubernamental y estándares internacionales, destinados a evitar que la inteligencia artificial ensanche brechas sociales y se asuma como disciplina de una nueva ingeniería centrada en el ser humano. Este cambio radical de cuadrante implica un cambio radical en las bases éticas del pensamiento jurídico, académico, político y social, para hacerlo dentro de perspectivas éticas que mantengan coherencia entre un antes, un durante la transición hacia lo aplicativo, y un después sostenible para la condición humana. En breve la ética será un tema central de la informática y la IA reemplazará gran parte del hacer humano como se lo conoce, abriendo perspectivas que necesitan una nueva alfabetización del quehacer y pensar humano. Deberá ser una acción mancomunada entre empresa, Estado y Academia, acompañada del adecuado entrenamiento para el cambio de las fuerzas laborales. En la región iberoamericana el cambio deberá organizarse en conjunto, para consolidar un bloque que permita resistir el seguro embate de las potencias que ya están lanzadas a colonizar el mundo digital. Es decir, el universo.

El **Bloque V** referido a **“Comercio electrónico, protección del consumidor electrónico, Big data en el Marketing, nuevos Modelos de Negocios”**, directamente vinculado a la Economía digital, al intercambio de bienes y servicios en que el ser humano participa en la cadena productiva, contó con la participación de tres conferencistas.

La Abogada Ma. Laura Spina, es Magister en Ciencia de Legislación (Universidad Nal. Litoral (UNL), Docente: Facultad Regional Sta. Fe, Universidades :Tecnológica Nal. y de B. Aires (UBA) Expuso sobre **“Nuevos retos para proteger al consumidor en el mercado digital”**. Mencionó problemas que agrega el medio digital a esta franja de mercado: tributación, comercialización de bienes y servicios digitales, medios de pago, legislación aplicable, entre la que destacó: Resoluciones Mercosur 43/2000, y 21/2003, relativas a “Derecho de Información del Consumidor en las Transacciones Comerciales Efectuadas a través de Internet” cuya infracción se regula por la legislación de cada país, existiendo dificultades dadas sus diferencias. Respecto a protección de datos personales

solo las de Uruguay y Argentina se alinean a la Unión Europea. El jurista realiza en el ámbito empresarial: Redacción de Políticas de Privacidad, de Términos y Condiciones de Uso, Contrato entre la Plataforma y el Comercio, análisis de condiciones de la Plataforma de Pago. En equipo con tecnólogos se analizará Intervención de bots (inteligencia artificial, machine learning),etc., identificación biométrica y su incidencia en protección de datos personales, diseño legal de derechos intelectuales y relaciones asociativas. Entre los retos al jurista señala: 1. Operaciones desde cualquier lugar mediante móviles, estando de viaje, etc 2. Sin ley ni jurisprudencia respecto a tecnologías disruptivas, 3 Seguridad y protección de datos en Internet de las Cosas: tener en cuenta desde el diseño. 4. Blockchain y Smart-contract: certificación documental mediante estos procedimientos. En argentina se regulan por Decreto 182/2019. 5. Máquinas con capacidad de aprendizaje autónomo. Responsabilidad?: Según la jurisprudencia es la empresa que predispuso la tecnología. Se cuestiona si es responsabilidad objetiva o subjetiva o actividad riesgosa.

En **“Los nuevos modelos de negocios y la aplicación del principio de prevención de operaciones ilícitas. Desafíos y responsabilidades ”**la Escribana Graciela Cami, Máster Derecho de Internet y Nuevas Tecnologías(Instituto Campus Stella, España), Miembro Comisión Derecho Informático:Instituto de Investigación y Técnicas Notariales (IITN)(AEU), Uruguay, habló de nuevos modelos de negocios con uso de tecnología, que pueden beneficiar al usuario final si se fijan controles y reglas. Dijo que los países deben cumplir el Principio de Prevención y tener en cuenta la Recomendación Número 15 de GAFI sobre Nuevas Tecnologías (TIC), identificar y evaluar riesgos de lavado de activos y usar esas TIC para modelos nuevos o ya existentes, con precauciones para mitigar riesgos y evitar que las plataformas tecnológicas se usen para cometer ilícitos, lavar activos y/o financiar terrorismo. Los titulares de empresas administradoras de plataformas web de préstamos entre particulares, deben aplicar las políticas de prevención de lavado de activos, para evitar que sus modelos de negocios sean usados de instrumentos para operaciones ilícitas. Habló de normativa mexicana y refirió a la resolución uruguaya de noviembre 21 de 2018 (Circular 2307 de 23 noviembre de 2018) de Recopilación de Normas del Sistema Financiero, circular del Banco Central del Uruguay 2321 de 17 de enero de 2019.

La Ingeniera Ana Haydée Di Iorio, investigadora y docente UFASTA, Argentina, en conferencia sobre **“Diseño, implantación y gestión de laboratorios de informática forense”** mostró lo que está detrás de ese ámbito comercial de los negocios para proteger la veracidad de los hechos y apoyar la investigación en casos judiciales relacionados no solo con todo lo que tenga que ver con delitos informáticos cometidos por diversas razones, sino también los cometidos en el ámbito comercial de manera individual o grupal o de la ciberdelincuencia organizada, lo que podría darse también en relación a grandes empresas, incluso transnacionales. La prueba de los sucesos depende de estos laboratorios y sus niveles tecnológicos deben estar acordes a la materia investigada en todas sus etapas: diseño, implantación y gestión, las que son complementarias. En este sentido son transversales a todas las áreas que se investiguen, dado que van a los aspectos tecnológicos de los sistemas informáticos que se despliegan en dichas áreas de la sociedad.

En el **Bloque VI** relacionado a **Documentación, Notarios, Registros Públicos y Nuevas Tecnologías**, la conferencia del Escribano Adolfo Orellano Cancela, Director General de Registros, Uruguay, nos introduce en el estado actual del proceso de **“Informatización de los registros públicos. Implantación de uso de firma electrónica avanzada en la gestión registral”** un tema práctico de uso de las tecnologías al servicio de los derechos de las personas en el ámbito patrimonial y personal, mostrando el proceso que se está cumpliendo actualmente en los Registros Públicos de Uruguay, sistema de alcance nacional.

El Registro viene en un proceso de informatización que data de 1980 a la fecha, tiene la información digitalizada con los resguardos pertinentes de seguridad y se encuentra actualmente en la etapa de avanzar hacia la informatización de la gestión de inscripción de documentos en línea, vía electrónica mediante el uso de firma electrónica avanzada digital por parte de los usuarios, entre ellos los Escribanos uruguayos, ahorrando tiempo, recursos, esfuerzos y evitando los riesgos incluso de pérdida o extravío de documentos originales como títulos de propiedad de inmuebles y vehículos por ejemplo, que requiere la inscripción. Esto además del aceleramiento de trámites y abaratamiento de costos para el usuario de los servicios registrales, incluidos Abogados que inscriben embargos, cancelaciones de los mismos y demás actos inscribibles y Escribanos como mencionamos que inscriben títulos de propiedad, hipotecas, cancelaciones, arrendamientos, etc.

En este mismo Bloque VI la conferencia sobre **“Entidades de Confianza”** de la Abogada Jimena Hernández, Ingeniero Jorge Prego y Abogado Matías Jackson, integrantes de la Unidad de Certificación Electrónica (UCE) de la Agencia estatal para la Gestión del Gobierno Electrónico y la Sociedad de la Información y el Conocimiento (AGESIC), nos introdujo en el análisis de estas Entidades relativamente nuevas en el Uruguay, reguladas por el Decreto 70 de 2018. Los disertantes nos informaron de primera mano los avances y aplicaciones prácticas que se pueden realizar relativos a la firma de documentos electrónicos con la firma electrónica avanzada, la de mayor valor probatorio y por lo tanto con fuerza de documento público solo sometida a tacha de falsedad, con relación a la firma misma, aún cuando en el área contractual no se descartan las posibilidades de ejercicio de acciones por error, violencia, dolo relativas al firmante o falta de solemnidad que se requiere legalmente en ciertos casos.

La Conferencia **“Plataforma de gestión de documentos públicos digitales notariales Provincia de Buenos Aires Argentina”** del Esc. Néstor Lamber, Miembro Academia Argentina Notariado, Direct. Diplomatura Univ. Notarial Argentina, Prof. Postgrado Derecho Inmobiliario Univ. Nal La Plata, Secretario Asuntos Legales y Documentación Digital: Colegio Escribanos Prov. B.Aires, Vocal Supl: Com.Directiva de Blockchain Federal Argentina describe la Plataforma de gestión de documentos públicos digitales en la Provincia de B. Aires que permite a los Notarios del Colegio de la Provincia de Buenos Aires en soporte digital realizar actuaciones notariales cumpliendo el Plan Estratégico de modernización de la Administración Pública, dado que si bien el Notariado ni el Colegio de Escribanos son parte de la Administración Pública Provincial, dada la potestad fedante del Notario por delegación estatal y en su relación con la Administración Pública y de Justicia provincial se impone la adecuación se reglamentaron las actuaciones notariales para soportes digitales de acuerdo a la ley 25.506 de Firma Digital con el mismo valor legal que

los documentos firmados en soporte papel, habilitando la realización en soporte digital de certificaciones de copias digitales de documentos digitales o en soporte papel digitalizados, copias o testimonios digitales de escrituras matrices, copias simples digitales y certificaciones de firmas digitales y se creó una plataforma a tales fines a cargo del Colegio de Notarios de la Provincia de Buenos Aires. El Folio de actuación digital podrá contener un código QR que permita recuperar la reproducción del contenido del documento digital.

El **Bloque VII**, sobre **Acceso a la información pública, justicia abierta, informática Forense**, se inicia con la Conferencia **“Del poder judicial electrónico a la justicia abierta: conceptos, evidencia y explicaciones”** dictada por José Miguel Busquets, Doctor en Ciencias Políticas, Universidad Cândido Mendes de Brasil. Docente en la Facultad de Ciencias Sociales de la Universidad de la República, Uruguay nos ilustró a través de su exposición con estadísticas y datos precisos sobre el tema en cuestión, desde el punto de vista de su especialidad, con una óptica diferente, útil para lograr una visión más completa del proceso que enfoca hacia una justicia abierta.

La conferencia **“Educando juristas para el siglo XXI”** de la Abogada María Luisa Tosi, Directora Jurisprudencia, Suprema Corte Justicia relató el proceso en Uruguay: el Estado desarrolla Políticas Públicas, impulsa condiciones para que las Instituciones implementen la inclusión social digital. Describe el trabajo de AGESIC (Agencia Gubernamental) desde 2005 y su control de cumplimiento en "Agendas Digitales" e inversiones en infraestructura: cable submarino de fibra óptica en 2017, etc). En inclusión menciona: planes CEIBAL e IBIRAPITÁ, para escuelas y adultos mayores respectivamente. Destaca la capacitación CEIBAL en Inteligencia Artificial: se crearon tres invenciones de utilidad práctica, dos premiadas en Houston y California respectivamente (hologramas e inteligencia artificial, que alivia el estrés de los astronautas y "CarAGUAta" que atiende déficit hídrico en huerta y la tercera: vehículo autónomo que esparce cal mitigando lectopirosis. En la Universidad se desarrolló la plataforma de Enseñanza EVA (Entorno Virtual de Aprendizaje) para grado y posgrado: permite actividades semipresenciales. En Facultad de Derecho, la mayoría de asignaturas Plan 2016, tiene al menos un curso semipresencial. En Poder Judicial se capacita a Magistrados, Aspirantes y Defensores, y otros desarrollos. 80% de cursos es a distancia; hay formación continua en la Plataforma ZOOM. La "Base de Jurisprudencia Nacional", con herramientas de la Inteligencia Artificial fruto de un Acuerdo específico, con la Cátedra de Lenguaje Natural, en el marco del Convenio entre la Corte de Justicia y Facultad de Ingeniería (UdelaR), para mejorar tareas: artesanales, anonimización de datos sensibles y estructuras de búsqueda. En Procesos de Enseñanza – Aprendizaje, los avances y desarrollos específicos, determinaron Instituciones competentes a capacitar, desarrollar e implementar herramientas propias, adecuadas a sus circunstancias y necesidades, en lo privado y lo público, con diferentes ritmos y avances.

El Ing. Roberto Giordano Decano y Docente de Ingeniería en la Universidad FASTA, Argentina, dictó la Conferencia **“Impacto de las investigaciones universitarias. Reflexiones desde la experiencia de la Universidad FASTA”** en la que desarrolló cinco puntos: 1. el Rol de la Universidad en la Era del Conocimiento. 2. La experiencia de la Fac.

Ingeniería (FI) en UFASTA. 3. Algunos Proyectos en FIUFASTA. 4. Buscando Impacto de la Investigación y 5. Reflexiones finales. En puntos 1 y 2. cita a Federico Mayor Zaragoza: la Universidad tiene una función preventiva y práctica, deber de anticipación global y papel activo en la sociedad para enfrentar nuevas necesidades sociales y ambientales, de ayudarla a diseñar el futuro nacional y regional, mejorar calidad de vida, ser dueños de su destino; se requiere nueva visión de la educación y medidas audaces e innovadoras (Declaración Foro Mundial de Educación 2015) Cita el marco normativo argentino. 3. Presenta algunos proyectos de FIUFASTA de tecnología aplicada: relacionado al cuidado de la salud: Proyecto VIHDA (Plataforma tecnológica del Programa Nacional de Vigilancia de Infecciones Hospitalarias De Argentina): en el primer año de aplicación se salvaron 500 vidas y ahorraron más de 4 millones de dólares. Hoy tienen un grupo interdisciplinario con 5 proyectos en marcha, 10 premios nacionales e internacionales y 4 declaraciones legislativas. La Resolución 680/18 (6.12.2018) aprobó Directrices para Programas de Prevención y Control de Infecciones Asociadas al Cuidado de la Salud (IACS) y la Resolución Ministerial 178/18 aprobó la Plataforma Oficial del Ministerio de Salud para evaluación, prevención y control de IACS. En esa base el Proyecto PAIF PURI en el Laboratorio de Informática Forense y la Guía para el Proceso Penal, al Programa INVESTIGA, permitió detectar delitos con estupefactantes e INVESTIGA, que permitió frustrar amenazas de bomba. 5. Entiende que en un mundo interconectado se puede realizar trabajos conjuntos y aplicar investigación más desarrollo (I+ D); que la universidad trabajando junto a la sociedad resulta útil y contribuye a solucionar problemas sociales.

Resumen de trabajos presentados

En el **Bloque I** titulado **“Gobierno digital. Derecho a la verdad. Desafíos”** se presentaron los siguientes trabajos:

el trabajo **“Fake news y Estado demorático: análisis de proyectos de ley y de las medidas que vienen siendo tomadas en Brasil y Argentina”** trata tema de actualidad. Sus autoras son la Ingeniera Ana Haydée di Iorio y la Abogada Tatiana Stroppa, Docentes e Investigadoras, respectivamente de Universidad FASTA, Argentina y Centro Universitario Bauru, Brasil. Entienden relevante elaborar indicadores que permitan al ciudadano detectar la veracidad de noticias y analizar filtros automatizados usados por las plataformas para retirar contenidos o dificultar su acceso, basados en algoritmos o mediante “sellos de chequeo”, pero eso puede ser censura privada y restringir pluralidad de voces y periodismo independiente. Al definir *fake news* (FN) citan varios autores, entienden que el término refiere a desinformación o a noticias falsas o fraudulentas, producidas con intención de provocar daño, que tienen tres elementos: falsedad, dolo y daño.

Analizan filtros automatizados usados por plataformas como Google y Facebook para retirar contenidos, basados en algoritmos o bloqueadores lo que entienden constituye una especie de censura privada. Respecto a proyectos de ley dicen las autoras que existen desde 2015 en Unión Europea, donde para los expertos lo importante es la alfabetización mediática a periodistas y ciudadanos para eliminar las FN.

En Brasil hay 15 proyectos de ley, con definiciones vagas, unos dirigidos a criminalizar, dando respuesta punitiva y otros determinando la remoción inmediata por las plataformas, promoviendo cambios en el Marco Civil de Internet y el Código Electoral. Hay garantía del derecho de informar y editorial, pero es difícil medir qué es información “perjudicialmente incompleta” sin contrariar las libertades de información y editorial y por el principio constitucional de legalidad se requiere ley previa, escrita y cierta para definir tipos penales. El reglamento de propaganda electoral en Internet (resolución 23551/2017) permite a partir del 16 de agosto del año de la elección, limitar la libre manifestación del elector identificado o identificable en Internet solo cuando hay ofensa al honor de terceros o divulgación de hechos sabidamente falsos.

En Argentina se presentó un proyecto de ley en 2018 con el objeto de crear una comisión de verificación de Noticias Falsas formada por periodistas y académicos para detección, reconocimiento, rotulación y prevención de notificaciones falsas difundidas por medios digitales durante las campañas electorales. Cuando dicha comisión encuentra una noticia falsa debe comunicar a la Cámara Nacional Electoral que puede ordenar a proveedores de internet que rotulen la noticia como de dudosa credibilidad, requerir a los proveedores de internet reducir la distribución de la noticia catalogada así, y registrar en la página web, creada por la Cámara Nacional Electoral que será de libre acceso, como noticia de dudosa credibilidad. El incumplimiento de dichas medidas en un plazo de doce meses genera multas, inhabilitación por 10 años en el Sistema de Proveedores del Estado o suspensión por dos años del portal o red denunciados que no levante el contenido falso o malicioso.

En el Bloque II : Derechos Humanos, protección de datos personales se presentaron dos trabajos:

María del Pilar Guzmán Cobeñas, Docente, Universidades César Vallejo y Nacional del Callao e Instituto Nacional de Derecho y Nuevas Tecnologías INDTEC, Perú expuso su trabajo **“Dos fundamentos del Derecho al Olvido Digital: La prescripción y la jerarquización de los datos informáticos en Internet”** Entiende necesario y propone el reconocimiento del derecho al olvido en la Constitución (Artículo 2 inc.5 y 6), en protección del Derecho a la intimidad consagrado en la misma, que es un derecho a la privacidad de datos de los ciudadanos y la información sobre ellos en Internet. Analiza un caso administrativo y jurisprudencial dado en Perú en que se solicita desindexación de la información que permanecía visible aunque se le reconoció ausencia de culpa y responsabilidad; solo luego de recurrir a tribunales de EEUU logró que retiraran de resultados de búsqueda la noticia que lo perjudicaba. Como el Derecho al Olvido no es reconocido por la Constitución sino por el órgano administrativo de protección de datos de su país, propone los dos fundamentos del título como base jurídica para la aplicación de este derecho: la prescripción de los datos y la jerarquización de los datos informáticos en Internet de acuerdo a la pirámide de la información de Rowley los cuales desarrolla más ampliamente en el trabajo.

Según Natasha Alves, Abog. Master U. Católica R. G.do Sul, Cristiano Colombo, Doctor en Derecho, igual Universidad y José Gaziero, Abog.Docentes e Investigadores (Brasil), en **“Da Economia do Compartilhamento e a proteção de dados pessoais em termos de aplicações**, la economía del compartir, fenómeno tecnológico surgido en 1995 junto a negocios en línea mediante portales que dieron herramientas para un sistema basado en intercambio de bienes o servicios, generaron comunidades de beneficio mutuo y confianza, garantía de sostenibilidad del modelo de negocio. Analizan aplicativos como UBER, refieren a Ley 12965/14 (marco civil de Internet), promotor de principios, garantías, derechos y deberes del uso de Internet en Brasil, la Ley General de Protección de Datos, 13709 de 2018, (vigencia febrero/2020) y estiman: a) respetar conceptos y principios fijados en la ley mejorará la protección de datos como derecho fundamental. b) los operadores del derecho deben considerar los beneficios aportados a la sociedad y evitar interpretaciones que debiliten esta economía. c) hay que considerar el derecho a la protección de datos, "vulnerabilidad del consumidor", "externalidad social negativa" derivada del "costo-tiempo de la lectura" de las políticas de privacidad, aplicar principio de finalidad al tratamiento de datos. Concluyen que en época de mercantilización de información, los datos personales e informaciones deben usarse para bien de la sociedad.

En el **Bloque III** se presentaron los siguientes trabajos:

En el trabajo **“Prevención y persecución de ciberdelitos: un nuevo terreno para la inteligencia artificial?”** Joselina Pastorini, Abogada, Docente, Adj. Derecho Penal en Universidad La Plata, Argentina, menciona dificultades en prevenir e investigar delitos informáticos, propone la implementar sistemas de Inteligencia Artificial (IA) para combatir el cibercrimen. Menciona países que implementaron sistemas con fines preventivos y/o investigativos – España, Holanda, Estados Unidos, para evaluar su aplicación en países de América Latina, como Argentina y Uruguay. **Concluye** que los delitos informáticos, por su “no convencionalidad”, rapidez en su ejecución y expansión en el “Ciberespacio” requieren mecanismos tecnológicos, rápidos y eficaces, nuevas herramientas que garanticen su prevención y persecución y mecanismos de prevención e innovación en investigaciones policiales y judiciales, y cree que IA es un mecanismo acertado pero para ser eficaz, debe acompañarse de instrumentos con el respeto a la legalidad y derechos fundamentales, evitando abusos y malas prácticas.

“Forensia de Internet de las cosas (IoT), avances en la investigación” trabajo los Ings. Beatriz Gallo, E. Rivetti, A. Gamarra y J. Aráoz, Docentes e Investigadores, Fac. Ingeniería, Univ. Católica, Salta, Argentina y la Abogada Bibiana Clara. Aborda el problema generado por Internet de las Cosas (IoT) y los avances del Grupo de Forensia Digital de la UCASAL.- IoT se define como “... conjunto de tecnologías enfocadas a permitir la conexión de objetos heterogéneos a través de diferentes redes y métodos de comunicación..” principal objetivo: posicionar dispositivos inteligentes en distintos lugares para capturar, guardar y administrar información y que sea accesible a personas desde cualquier parte..” “ Internet móvil, permite rápida alfabetización digital de millones de personas, habilita una sociedad inclusiva y sostenible, pero el software malicioso permite robar datos, interrumpir el funcionamiento de sistemas, apoderarse de claves y contraseñas, causando daños que pueden afectar objetos conectados a IoT. Si éstos

cumplen tareas vitales o de alto riesgo los daños se potencian. Preocupan especialmente los sensores con cada vez mayores capacidades de captura, resguardo y transmisión de datos, la seguridad, características técnicas y funcionalidades. (electrodoméstico hogareño o dispositivos de control automático de señales, etc). A la fecha el equipo analiza los modelos de investigación para elegir el más apropiado: se seleccionaron 3 (Profit, ProbeloT y Falot). El equipo se propone: **Estudiar y analizar las políticas, normas y disposiciones sobre seguridad informática** vinculadas a dicho objeto de estudio. **Enfocar el estudio** desde el Derecho y la Informática. **Formular metodología de análisis forense para IoT** identificando componentes, funcionalidades, estructuras y características útiles a generalizar el método. IoT plantea **desafíos** a Forensia Digital: herramientas, protocolos de actuación y tecnologías forense poco aptas, gran cantidad de datos, que se siguen generando al momento de la investigación forense requieren más tiempo para identificación de la información relevante, su resguardo y preservación dado que no se pueden desconectar para aislarlos y preservar la prueba digital. El proceso de extracción de pruebas se puede complicar (los dispositivos IoT tienen formatos de datos heterogéneos, protocolos e Interfaces físicas involucradas). La diversidad de dispositivos, con sistemas operativos propietarios, y la creciente capacidad inteligente de los sensores y actuadores se suman a la problemática que en sí ya tiene la Forensia Digital: rigurosidad en la cadena de custodia, capacitación de analistas forenses en estas nuevas tecnologías, normalización y estandarización de los registros (logs) de eventos, normativa legal y jurisprudencia sobre el tema. Por otro lado las tecnologías informáticas cuya máxima expresión es IoT, resulta un ámbito muy propicio para el desarrollo del delito, dado que también se ha profesionalizado el uso de las TICs en el campo delictivo.

El Trabajo de la Ing. Informática Sofía Arancibia, Fac. Ciencias Hídricas UNL Argentina, **“Detección de creepware en computadoras personales mediante el uso de técnicas de ciberseguridad, análisis de datos”** propone el análisis de tráfico de red como método de detección de software malicioso (*malware*). Se enfoca en la detección de malware tipo *creepware* en computadoras personales (notebook, netbook, desktop), caracterizado por acceso ilegítimo a dispositivos de audio y video, y la exfiltración posterior de los datos capturados. Presenta el uso de métodos supervisados de aprendizaje automático (machine learning), para detección basada en clasificación de tráfico de red. Como parte del mismo se generaron datos de entrenamiento y pruebas mediante detonación, en entornos controlados, de diferentes ejemplares del malware. En los resultados se identificaron diferentes conjuntos de características aplicables al tráfico generado por el malware del tipo creepware, que permitieron clasificar y detectar ataques con una precisión por encima del 90%. La autora entiende esencial la clasificación de tráfico en internet para el manejo de grandes redes de datos y prevención y detección de infecciones en un dispositivo. También ve los métodos basados en protocolos y números de puerto incompletos hoy, por el uso de puertos reservados u otros, refiriendo a la clasificación de tráfico basado en estadísticas de gran interés actual, que implica aplicación de métodos de aprendizaje supervisado por modelos. Luego de su análisis técnico de pruebas y resultados concluye que los tres modelos que analizó lograron cumplir la tarea de forma correcta. Identifica tres aspectos a implementar en versiones posteriores: incorporar interfaz gráfica que facilite la ejecución del sistema a usuarios no familiarizados con la línea de comandos, brindar un mecanismo de rastreo de archivos y/o procesos

relacionados a la intrusión y extrapolar el desarrollo a dispositivos móviles con sistema operativo Android.

En el Bloque IV : “Inteligencia Artificial y Robótica” se presentaron los siguientes trabajos:

“No solo es un robot: rompiendo paradigmas jurídicos y redimensionando las relaciones personales” de Ana Karin Chavez Valdivia, Abogada, Docente, Universidad de La Salle, Perú, plantea el discutido tema de las relaciones sociales entre humanos y robots que enfrenta al problema de la responsabilidad del producto y a los cuestionamientos y temores fundamentados en amenazas y desafíos diversos entre ellos si un robot puede tener personalidad jurídica y ser sujeto de derechos y responsabilidades en sus relaciones sociales. Menciona el debate en la doctrina jurídica y la evolución hacia el reconocimiento de dos personalidades diferenciadas: las personas individuales y las colectivas. Cita la tesis de la voluntad de Savigny y la resolución del Parlamento Europeo de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión relativas a normas de Derecho Civil sobre robótica en que le pide realizar una evaluación de impacto y analizar las implicaciones de crear una personalidad jurídica específica para robots autónomos más complejos que sean responsables de reparar daños que causaren. Concluyendo, opina que la “personalidad” como concepto legal no surge de la humanidad del sujeto sino de la atribución de derechos y deberes al mismo. Entiende que una persona robótica o revestida de derechos y obligaciones y por tanto capaz de celebrar actos jurídicos de diversa naturaleza podría comprender, decidir y expresar la intención de celebrar un contrato matrimonial con un ser humano.

En el Bloque V : “Comercio Electrónico, Protección del consumidor electrónico, Big Data en el Marketing, Nuevos Modelos de Negocios” se presentaron los siguientes trabajos:

“Big Data marketing en el Mercosur, Protección de Datos y Normas de Seguridad” de los Licenciados Lía Bosque, A.Tondelli y Mag. Lic. Marco A.Villán, Docentes, Univ.Argentina de la Empresa (UADE) analizan la regulación de protección de datos personales y Big Data marketing (grandes cantidades de datos, estructurados, semi o no estructurados, recolectados para mejorar la relación con el cliente, optimizar resultados de la empresa y medir su fiabilidad) en los países fundadores del MERCOSUR (Argentina, Brasil, Paraguay, Uruguay). Analiza las normas de seguridad a cumplir por los responsables del tratamiento de datos con fines de mercadotecnia y compara con el Reglamento de Protección de Datos de la Unión Europea, y los conceptos de privacidad por diseño y por defecto que contiene. Las normas de seguridad a cumplir por las empresas que hacen Big Data Marketing deben reflejarse en medidas que resguarden confidencialidad y privacidad de datos personales y tener niveles básicos, medios y avanzados que aseguren que los datos no caigan en manos de terceros. El desafío para las empresas de marketing de Latinoamérica es muy amplio: por un lado deben adaptar sus políticas de privacidad y seguridad a la normativa Europa si realizan el tratamiento de datos de ciudadanos europeos, por otro estudiar y analizar políticas de

seguridad de la región e invertir en medidas de seguridad robustas, técnicas y organizativas que exigen las leyes del MERCOSUR. Refieren también a gobierno abierto y datos abiertos que habilita, al marco legal actual de la región, la necesidad de un esfuerzo conjunto para crear normativa unificada y exigir mayores medidas de seguridad.

“Hipervulnerabilidade do consumidor no ciberespaço e o tratamento dos dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais Brasileira (LGPD)” del Doctor Cristiano Colombo, Pos Doc PUCRS, Master y Abog. Guilherme Damasio Goulart, Brasil, Miembros Centro Estudios Jurídicos Investigadores, Brasil.

El trabajo aborda el tema de la hipervulnerabilidad del consumidor en el ciberespacio, sobre todo, involucrando las violaciones como consecuencia del tratamiento inadecuado de sus datos personales, a la luz de la Ley General de Protección de Datos (Ley nº 13.709 de 2018 - LGPDP). Su objetivo es reflexionar sobre las características del ciberespacio, analizando sus peculiaridades y la inserción del consumidor en este contexto, con exceso de información y escaso nivel de comprensión de informaciones técnicas, generando muchas veces al usuario o consumidor una gran inseguridad real o percibida.

La vulnerabilidad del consumidor (art. 4º, inc. I del Código de Defensa del Consumidor) es uno de los principios más importantes de protección del consumidor, que puede ser técnica, jurídica, fáctica o por la propia debilidad de ciertos consumidores según autores que citan; estas vulnerabilidades se agregan a la vulnerabilidad fáctica propia de la sociedad de la información, ya desde el acceso a la información del producto, a través de la publicidad y propaganda dado el marketing de los proveedores. La vulnerabilidad en la información se da desde dos puntos de vista: además del mencionado respecto al producto se refiere a sus datos personales, tema que también tratan los autores. Abordan el tratamiento de datos personales introducido por la Ley General de Protección de Datos Personales brasileña (LGPDP), para lo cual estudian la doctrina nacional y extranjera y la legislación nacional e internacional a fin de observar las dificultades con vista a los caminos a seguir en la práctica. Concluyen que el consumidor es hipervulnerable frente a las peculiaridades del ciberespacio, incrementando su debilidad, propulsando la evolución en la escalada de los niveles de vulnerabilidad, debiendo el ordenamiento jurídico acompañar y promover la protección de los datos personales de sus titulares.

En el Bloque VI “Documentación, Notarios, Registros Públicos y Nuevas Tecnologías” se presentaron los trabajos :

“Función Notarial y TICs Modernización del ejercicio de la profesión notarial” de la Esc. Silvana Rodríguez, sobre el uso de firma electrónica y documentos electrónicos en la función notarial, menciona la ley 18600 y la Acordada Reglamentaria 7831 de 2015 de la Suprema Corte de Justicia, que regula el uso de la firma electrónica avanzada en la función notarial y del soporte electrónico notarial para los documentos electrónicos y los documentos que puede realizar el Notario en dichos documentos aunque existen a la fecha algunos problemas operativos. También muestra aplicaciones en Oficinas y Registros Públicos de Uruguay.

En el trabajo **“Una aproximación a la Inteligencia Artificial IA) en el ámbito notarial”** Dde Beatriz Rodriguez Escribana,y Flavia Baladan, Abogadas, integrantes de ISOC (Internet Society), Abordan las principales características de la inteligencia artificial desde su concepto y forma de impactar en el Derecho. Analizan aspectos relativos al notariado, desde un punto de vista práctico. Respecto a la definición de IA, las autoras remiten a la del Autor español José Vida: *“Una rama de la informática que estudia y desarrolla sistemas capaces de realizar tareas propias de la inteligencia humana, en particular, comportarse de manera autónoma”*. Observan que en los últimos años hubo algunos avances en la gestión notarial: búsquedas en bases de datos normativas y jurisprudenciales como Jurisprudencia Nacional de la Suprema Corte de Justicia, las del IMPO, o el Poder Legislativo, también en el sistema automatizado de solicitud de certificados en los registros notariales, y realización de certificados electrónicos en soportes notariales electrónicos. Proponen aplicar IA a la Oficina Notarial en la elaboración de ciertos documentos (agenda de citas, minutas, formularios).

En el Bloque VII “Acceso a la Información Pública, Justicia Abierta, Informática Forense” se presentaron tres trabajos:

“Acceso a la información pública en la provincia de Buenos Aires, Argentina. Aporte al análisis de transparencia en América Latina” de María Fernanda Giaccaglia, Bibiana Luz, Abogadas Ing. Ana Di Iorio, Antonela D’Onofrio, Ruffa, María Belén; Uriarte, Verónica (Universidad FASTA y de Fraternidad de Agrupaciones Sto. Tomás de Aquino, Mar del Plata, B. Aires, Argentina) expresan; el derecho de acceso a la información pública es de toda persona a pedir información a sus representantes públicos para promover transparencia. Los Estados buscan sancionar leyes y adecuar sus portales institucionales, mediante tecnologías derecho. Analizan portales institucionales de poderes de la provincia B. Aires, basada en métricas del documento *Leffis Metric on e-government development* adaptadas a una herramienta analítica que proponen. La ley nacional Argentina 27275 de 2016 regula el Derecho, en Organismos y Poderes del Estado, empresas y sociedades estatales y entidades privadas y mencionan la Constitución, Convenciones, Normas y Tratados Internacionales aplicables. Relatan que tienen leyes las Provincias de B. Aires, Chubut y Río Negro entre otras pero el diagnóstico de 2017 de la Red Federal de Acceso a la Información Pública, constata que sólo en 9 jurisdicciones hay políticas de implementación sistemática de transparencia y acceso a la información. Proponen un dinámico cambio en las burocracias estatales en la producción de información de servicios y actividades públicas, para que se realice de forma proactiva, oportuna y sea fácil de encontrar, usar y entender.

“Aplicaciones de la tecnología blockchain en el área forense” Vicente Torres Zúñiga, Docente, Investigador, UNAM, Fac. Medicina. Licenciado en Ciencia Forense, México. El trabajo explica que la tecnología emergente llamada blockchain promete ser parte de procesos de certificación de documentos, transacciones y comunicaciones digitales, que ha usado con éxito como parte de esquemas de monedas digitales. Expresa sus

posibilidades para aplicarse en situaciones diversas de interés forense. Menciona las particularidades del indicio digital, describe las medidas de seguridad para evitar adulteraciones describe la tecnología blockchain en tanto protocolo informático y en términos técnicos, sus componentes y su funcionamiento mediante etiquetas de identificación y de seguimiento por bloques así como las medidas de seguridad que se usan en la creación de los bloques y en un sistema descentralizado de control del contenido de los bloques y del ingreso de nuevos bloques de información, menciona las particularidades del indicio digital, y da varios ejemplos de cómo puede ayudar a los peritos en informática para preservar el indicio digital, menciona posibles vías para que forme parte como cadena de custodia digital. Considera que es importante que el perfil profesional de los abogados conozca los alcances y aplicaciones que puede tener esta herramienta novedosa.

“ObE Forensics: una herramienta para el análisis forense de correos electrónicos”

Enzo Notario, Beatriz P. de Gallo Ingenieros. Docentes Fac. Ingeniería. Univ. Cat. Salta, y Marcela Vegetti, – Inst. Desarrollo y Diseño (Conicet/UTN), Sta. Fe. Todos :Argentina. El trabajo describe una herramienta informática de análisis forense de correos electrónicos, basada en una ontología, sus características técnicas y funcionales, el modo en que se integra en el procedimiento pericial de correos electrónicos y las primeras instancias de validación hechas por usuarios expertos- sobre el prototipo de la aplicación. Forense. Aporta rigor metodológico al trabajo pericial. Al basarse en una ontología, se garantiza que el modelo construido OntoFoCE responda a un método científico, genera un contexto de comunicación con los actores judiciales (jueces, abogados, otros peritos) basado en un mismo sistema terminológico y conceptual. Aplicando tecnologías semánticas se logró representar la trazabilidad del envío de un correo electrónico permitiendo avalar el carácter probatorio del documento digital y reforzando su capacidad de no repudio. ObE Forensic responde a los objetivos que persigue: representar la trazabilidad del proceso de transmisión e identificar los datos de las cuentas intervinientes. Aun así, es necesario atender las sugerencias de mejora aportadas por los usuarios expertos y continuar realizando pruebas de validación dado que pueden surgir nuevos puntos de pericia que no se puedan responder con las preguntas existentes hoy en ObE Forensic, por lo que es deseable contar con un editor de preguntas de competencia, para aprovechar al máximo la base de conocimiento que brinda y no limitar la aplicación a un conjunto cerrado de resultados. Otras líneas de investigación surgen de esta propuesta, considerando que la tecnología avanza en el desarrollo de nuevas áreas (Internet de las Cosas, Inteligencia Artificial) que requieren el trabajo interdisciplinario como el Derecho y la Informática.