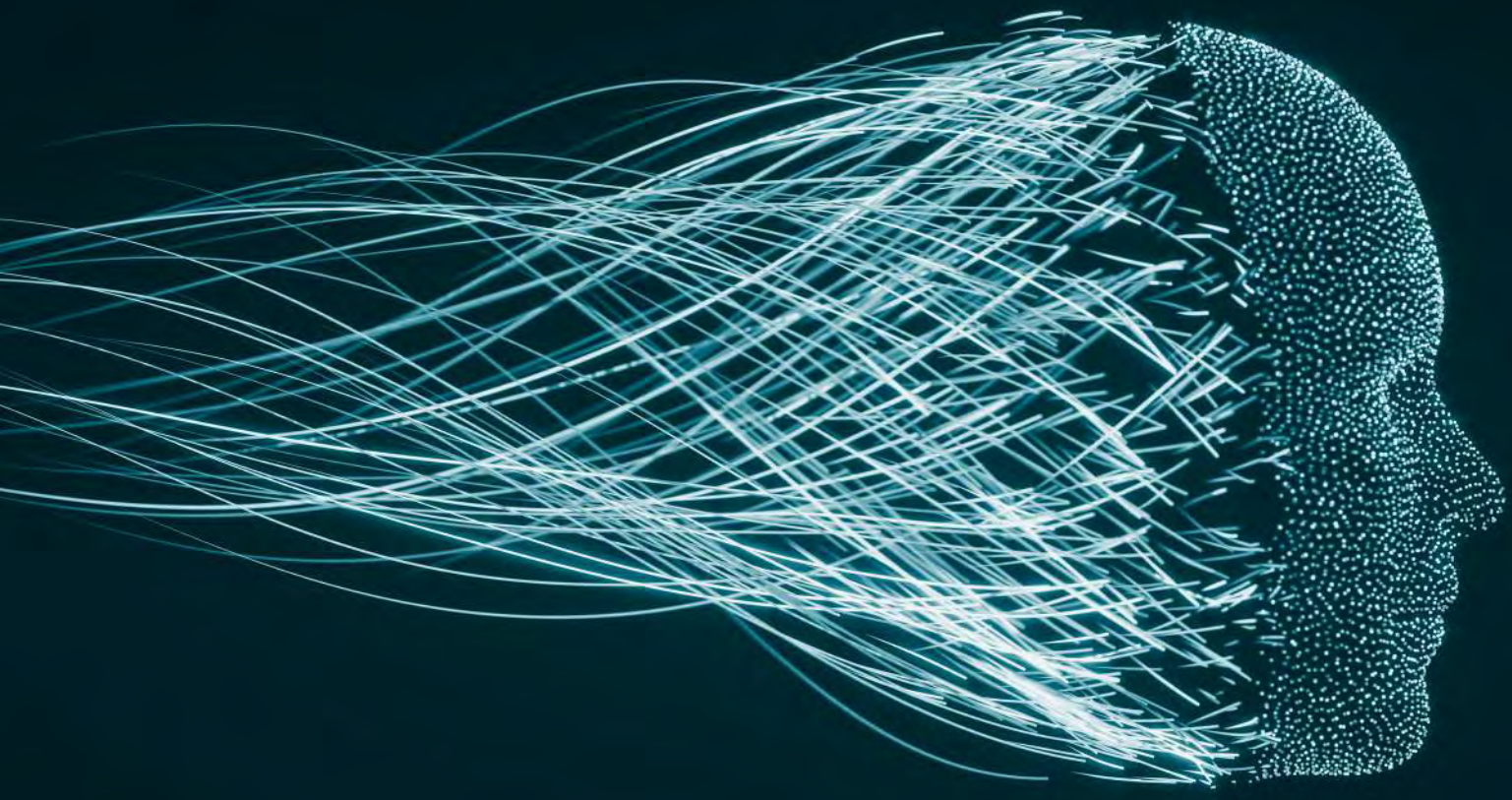
Nº1 **DIC 22**

LAWCEDIC



OCEDIC

UNIVERSIDAD AUSTRAL | DERECHO

NOTA AL LECTOR

Este trabajo ha sido elaborado a partir de datos seleccionados durante el período comprendido entre junio de 2022 y principios del mes de diciembre de 2022. Dado el carácter dinámico de nuestro objeto de estudio, así como del marco normativo de cada país y, ante la constante creación, modificación y desaparición de contenidos en Internet, se recomienda al lector que desee citar esta publicación que verifique, a la hora de hacerlo, si la información exhibida requiere actualización.

El presente documento no pretende ser un asesoramiento legal para el usuario. El mismo fue realizado como una guía que centraliza material encontrado y destacado por el equipo académico de LawCedic. En consecuencia, los listados de jurisprudencia y legislación no son taxativos.

PRÓLOGO

Profunda emoción nos genera ser partícipes de la evolución del Observatorio de Cibercrimen y Evidencia Digital de la Universidad Austral (OCEDIC). Pero no solamente por su expansión a casi todas las provincias de la República Argentina y países de la región, sino también por el ingreso incesante y constante de tantos abogados, jueces, fiscales, ingenieros, psicólogos, informáticos, técnicos y jóvenes profesionales que hoy forman parte de esta maravillosa comunidad.

OCEDIC fue pensado y creado como un espacio para todos. Y con mucha dedicación, perseverancia y profesionalismo, un gran equipo, que al principio éramos unos pocos y hoy superamos los 100, fuimos desarrollando para vos tantas actividades y proyectos novedosos, que hoy no podemos dejar de seguir generando propuestas únicas, diferentes; detectando las necesidades de quienes nos siguen –una comunidad de más de 20.000 personas que conforman nuestro Club OCEDIC escuchando las propuestas de todos, y haciendo realidad un sueño: un espacio cada vez más y más grande de todos y para todos.

Sin dudas, un equipo cuyos integrantes nos identificamos en tres aspectos: la pasión, el profesionalismo y la necesidad de innovar siempre, y juntos, logramos que OCEDIC haya trascendido, que tenga vida propia y que haya superado todas las expectativas.

Y así nace LawCedic; de la mano de su Team Leader Denise Gross y un excelente equipo, que ha desarrollado este maravilloso proyecto que despega hoy para toda nuestra comunidad.

El objetivo de LawCedic no es únicamente acercarte, en un solo lugar, el excelente trabajo de compilación sobre lo último en cibercrimen y evidencia digital (jurisprudencia, legislación, ensayos, comentarios a leyes y más), sino también, que vos mismo seas parte de este viaje.

¿Cómo? escribinos a lawcedic@gmail.com. podés enviarnos tu propuesta para escribir un ensayo y que sea publicado a lo largo de las diferentes ediciones, o enviarnos material (jurisprudencia, informes, legislación, etc.) que creas que no puede faltar en próximos suplementos. Tu aporte es fundamental. Sumate.

La unión nos hace grandes y fuertes. El lugar ya lo tenemos: OCEDIC.

DANIELA DUPUY
DIRECTORA OCEDIC

CATALINA NEME
SUBDIRECTORA OCEDIC

PRESENTACIÓN

La lucha contra el cibercrimen evoluciona de manera constante. Esto representa un desafío, no solo desde un punto de vista técnico, ante el avance de nuevas tecnologías, sino también desde el plano jurídico, cuando los operadores del derecho deben hallar la respuesta adecuada frente a una determinada situación y se encuentran con una gran cantidad de normas y textos dispersos, no siempre actualizados.

Asimismo, el sector académico se enfrenta a la necesidad de lograr que las publicaciones se mantengan "vigentes" cuando sabemos que, realizar una investigación o explorar un objeto de estudio y, luego, presentar seriamente un resultado, lleva mucho tiempo.

Desde el Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales de la Universidad Austral (OCEDIC), un espacio de intercambio y de cooperación entre múltiples partes interesadas, se fueron generando iniciativas para poder acompañar, orientar a los distintos sectores e incluso fomentar cambios que sirvan para encontrar soluciones más eficientes ante un fenómeno multiforme y transversal como es el ciberdelito. De estos proyectos han surgido publicaciones, capacitaciones y eventos, en Argentina y en otros países.

Además, el Observatorio envía periódicamente a los interesados un Newsletter, que nació con la finalidad de proponer una fuente de lectura ordenada, luego de una selección (entre la gran cantidad de información que circula por Internet), de noticias relevantes de diversa índole, siendo el cibercrimen y la evidencia digital el hilo conductor. Las mismas son previamente verificadas por un equipo y se dirigen a un público variado, interdisciplinario, con mayor o menor expertise en el área. En este documento los contenidos se dividen por categorías bien visibles para que cada suscriptor pueda decidir lo que tiene ganas de leer o no. En consecuencia, es posible acceder a notas de actualidad, novedades jurídicas, publicaciones institucionales y académicas, libros, una agenda con cursos y eventos y hasta un glosario. Aun así, incluso unas horas después de haberlo enviado, hemos llegado a identificar material pertinente que aparece y que nos gustaría incorporar, lo que resulta frustrante y fascinante a la vez, confirmando la importancia de mantenerse actualizado frente al riesgo permanente de obsolescencia.

La realización de todas estas tareas exige búsquedas pormenorizadas, recorriendo una gran cantidad de bases de datos e innumerables consultas por Internet. En este contexto, fue posible detectar la falta de un boletín, suplemento o instrumento que centralice los avances en la normativa y la jurisprudencia, a nivel nacional e internacional. Consideramos que una publicación que esté exclusivamente dedicada al mundo jurídico podría ser de suma utilidad para aquellos que necesitan aplicar las leyes cotidianamente, dado que pueden contar con una herramienta complementaria, un back-up que se puede tener a mano cuando hace falta encontrar, por ejemplo, un fallo sobre un tema determinado.
Y así nació LawCedic.

LawCedic es el resultado de la reunión de un equipo compuesto de abogados, fiscales, jueces y profesionales del derecho que buscan aportar su granito de arena, a través de la selección, análisis, condensación y divulgación de herramientas jurídicas relacionadas con los cuatro ejes del Observatorio: ciberacosos a niños, niñas y adolescentes; violencia de género digital; ataques informáticos y fraude; inteligencia artificial, herramientas disruptivas en investigaciones criminales y metaverso.

En dos años el OCEDIC ha conseguido dar a conocer su trabajo en España y en América Latina, lo que nos lleva a intentar ir sumando elementos de derecho extranjero, comparado e internacional. Esto nos parece indispensable, principalmente, a la hora de abordar una temática transfronteriza, que requiere un nivel de cooperación internacional superior a otros tipos de criminalidad.

Por otro lado, creemos que una reseña de legislación y jurisprudencia no sería suficiente porque nuestro equipo se destaca por las ganas de desarrollar contenidos que sean el fruto de sus propias reflexiones inéditas. LawCedic aspira a proporcionar también un aporte sustancial en otra gran fuente del derecho: la doctrina. Se pretende elaborar ensayos, comentarios de fallos y artículos propios. Para ello, trabajarán sus miembros y se abrirán convocatorias para publicación.

En síntesis, LawCedic desea brindar a los especialistas un documento especial, cada tres meses, que puedan consultar cuando estén buscando un compendio con legislación que incluya avances normativos, jurisprudencia, aportes doctrinarios y comentarios sobre temas de vanguardia que van a enriquecer debates e investigaciones y, con suerte, remover algunos de los obstáculos existentes en la toma de decisiones.

¿LawCedic es un boletín? ¡No! :) ¿Es un suplemento ? Mmmm sí y no... ¡¡¡¿¿¿Qué es LawCedic???!!! Es LawCedic...

Como todo lo que sucede en OCEDIC, LawCedic no es una estructura rígida, podrá ir mutando y mejorando con el tiempo. Por lo pronto, esperamos con ello crear nuevos puentes entre el público del OCEDIC, ayudar a quienes se levantan todos los días con la enorme responsabilidad de proteger a la sociedad y a las víctimas de la ciberdelincuencia, armonizar respuestas, despertar y mantener el interés de quienes hagan clic para ver nuestro material, así sea por curiosidad.

Para terminar, sabido es que no se puede crear y ejecutar un proyecto sin el apoyo de mentes visionarias y apasionadas. Un gran agradecimiento a las autoridades del OCEDIC, Daniela Dupuy y Catalina Neme, a los colaboradores, al equipo de edición, a los diseñadores y, por supuesto, a los lectores.
Sin ustedes, esto no sería posible.

Buena lectura.

DENISE GROSS
TEAM LEADER

ÍNDICE

SIGLAS Y ABREVIACIONES

AAIP	Agencia de Acceso a la Información Pública de Argentina
ACLU	American Civil Liberties Union
AEPD	Agencia Española de Protección de Datos
AFIP	Administración Federal de Ingresos Públicos (Argentina)
art./arts.	artículo/artículos
BCRA	Banco Central de la República Argentina
BO	Boletín Oficial
BOE	Boletín Oficial del Estado (España)
c/	contra
CABA	Ciudad Autónoma de Buenos Aires
CJ	Circunscripción Judicial
CEPD	Comité Europeo de Protección de Datos
CN	Constitución Nacional
CNCC	Cámara Nacional de Apelaciones en lo Criminal y Correccional
CNCP	Cámara Nacional de Casación Penal
CNIL	Commission nationale de l'informatique et des libertés
COE	Consejo de Europa
CP	Código Penal
CPCC	Código Procesal Civil y Comercial
CPJRC	Código Procesal para la Justicia en las Relaciones de Consumo
CPPN	Código Procesal Penal de la Nación
CRA	Cyber Resilience Act
CSJN	Corte Suprema de Justicia de la Nación
DMA	Digital Markets Act
DNI	Documento Nacional de Identidad
DPC	Data Protection Commission
DSA	Digital Services Act
EDPB	European Data Protection Board
EE.UU.	Estados Unidos de América
ENACOM	Ente Nacional de Comunicaciones
expte.	expediente
FINTECH	Financial Technology
func.	funcionamiento
GPS	Global Positioning System
IA	Inteligencia Artificial
ICBC	Industrial And Commercial Bank of China

IFE	Ingreso familiar de emergencia
inc.	inciso
IoT	Internet Of Things
IP	Internet Protocol
JEPD	Junta Europea de Protección de Datos
LOPMI	Loi d'Orientation et de Programmation du Ministère de l'Intérieur
MASI	Material de Abuso Sexual Infantil
MiCA	Markets in Crypto-Assets
MPF	Ministerio Público Fiscal
MPIL	Meta Platforms Ireland Ltd.
N°/Nro.	Número
NACDL	National Association of Criminal Defense Lawyers
NIS	Network and Information Security (directiva)
OCEDIC	Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales
O.D.I.A.	Observatorio de Derecho Informático Argentino
OSINT	Open Source Intelligence
p. /ps.	página/ páginas
párr./párrs.	párrafo/párrafos
PPJCyF	Penal, Penal Juvenil, Contravencional y de Faltas
Res.	Resolución
RGPD	Reglamento General de Protección de Datos
s/	sobre
S.A.	Sociedad anónima
SEPD	Supervisor Europeo de Protección de Datos
SMS	Short Message System
S.R.L.	Sociedad de Responsabilidad Limitada
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
T-CY	Comité del Convenio sobre la Ciberdelincuencia
TEDH	Tribunal Europeo de Derechos Humanos
TICs	Tecnologías de la Información y de la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
UE	Unión Europea
vs.	versus


JURISPRUDENCIA

JURISPRUDENCIA

Este espacio tiene como objetivo presentar una colección de sentencias dictadas desde fines de junio de 2022 hasta el presente[1], vinculadas con cibercrimen y evidencia digital, en especial, con los ejes del OCEDIC, que pueden ayudar al lector a la hora de interpretar y aplicar las normas en casos concretos a nivel nacional (derecho argentino) e internacional. Cabe señalar que los colaboradores han tenido la intención de dedicar una mayor cantidad de líneas a los fallos que consideran destacados.

CIBERACOSOS A NIÑOS, NIÑAS Y ADOLESCENTES

ARGENTINA

GROOMING.

EXPLOTACIÓN SEXUAL INFANTIL.

PRODUCCIÓN DE MATERIAL DE ABUSO SEXUAL INFANTIL.

TRIBUNAL ORAL EN LO CRIMINAL FEDERAL N° 6 - EXPTE. N° CFP 18639/2017/TO1 - 12/08/2022.

Se condenó a dos personas por considerarlos coautores penalmente responsables del delito de trata de personas con fines de explotación configurada mediante la promoción, facilitación y comercialización de material de abuso infantil, agravado por haberse concretado dicha finalidad y por haber sido cometido mediante engaño y aprovechamiento de la situación de vulnerabilidad de las víctimas. La sentencia tuvo por acreditado que los acusados contaron con todo el instrumental necesario para realizar la actividad ilícita que se les imputó y que ambos tenían montada una estructura a esos fines. Asimismo, se puntualizó que se le otorgó relevancia convictiva a la declaración de una de las víctimas siendo dicha prueba acompañada por el plexo probatorio producido en la causa que, analizada de acuerdo a la sana crítica racional, las reglas de la lógica y la experiencia común, permitió verificar la veracidad de su relato.

ACCEDER

ARGENTINA

GROOMING.

CIBERACOSO.

CONTACTO VÍA *WHATSAPP.*

JUICIO ABREVIADO.

JUZGADO DE CONTROL DE GENERAL PICO, PROVINCIA DE LA PAMPA - EXPTE. N° 69010/2022 - "M.,P.F. C/ S., J. M. S/ CIBERACOSO" - 16/08/2022.

Se condenó a J.M.S. por considerarlo autor material y penalmente responsable del delito tipificado por el art. 131 del CP. Se tuvo por acreditado que el imputado mediante la aplicación de mensajería instantánea WhatsApp se comunicó con P. B. S. C. de 14 años de edad, quien fuera hija de su pareja R. C., con el propósito de mantener un contacto de tipo sexual.

ACCEDER

[1] Excepcionalmente, este primer número contiene elementos seleccionados en el último semestre. Los próximos serán ediciones trimestrales.

ARGENTINA

GROOMING.

ABUSO SEXUAL AGRAVADO.

CORRUPCIÓN DE MENORES.

PRODUCCIÓN DE MATERIAL DE EXPLOTACIÓN SEXUAL INFANTIL.

JUICIO ABREVIADO.

CÁMARA EN LO CRIMINAL Y CORRECCIONAL DE LA CUARTA CIRCUNSCRIPCIÓN JUDICIAL DE LA PROVINCIA DE CÓRDOBA, VILLA MARÍA - EXPTE. N° 9930390 - "B. B., R. F. - P.S.A. DE GROOMING, ETC." - 30/08/2022.

Se condenó a R.F.B. a 10 años de prisión, accesorias de ley y costas por considerarlo responsable del delito de grooming; promoción a la corrupción de menores de 18 años de edad; producción de material de abuso sexual de menores de dieciochos años de edad; abuso sexual con aprovechamiento de la inmadurez sexual de la víctima agravado por el peligro de contagio de enfermedad de transmisión sexual; tenencia de representaciones sexuales de menores de 18 años de edad reiterada, contra 14 menores de edad. Las conductas enrostradas se circunscribieron a una serie de acciones deliberadas, a través de vías tecnológicas y redes sociales, con el fin de ganarse la confianza o amistad de los menores de edad -cuyas edades conocía-, generando una conexión emocional con ellos con el objeto de llevar a cabo actos sexuales perseguidos penalmente.

ACCEDER

ARGENTINA

GROOMING.

ABUSO SEXUAL.

EXPLOTACIÓN SEXUAL INFANTIL.

JUICIO ABREVIADO.

FORO DE JUECES PENALES 3° CJ BARILOCHE, PROVINCIA DE RÍO NEGRO - EXPTE. N° MPF-BA-01091-2022 - G.,A.N. C/ G.,R. Y S.,J. NN S/ PRODUCCIÓN Y DISTRIBUCIÓN DE IMÁGENES DE ABUSO SEXUAL INFANTIL" - 13/09/2022.

Se condenó a S.J.G. a 10 años de prisión por el abuso de una menor de 10 años. Las conductas imputadas comenzaron cuando el acusado contactó a la víctima a través de la aplicación de mensajería instantánea WhatsApp e inició un intercambio de mensajes e imágenes de contenido sexual, maniobras que fueron facilitadas por el aprovechamiento de las condiciones de discapacidad de la madre de la menor, quien sufre de "episodios de descompensación psicótica y presenta un compromiso en su capacidad intelectual de tipo límite".

ACCEDER

ARGENTINA

GROOMING.

JUICIO ABREVIADO.

TRIBUNAL EN LO CRIMINAL N°3 VOCALÍA 8 DE LA PROVINCIA DE JUJUY - EXPTE. N° 4959/2022 - "N. F. E. P.S.A. DE GROOMING. PALPALÁ" - 16/09/2022.

Se condenó a F.E.N. a una pena de prisión de 2 años y 6 meses de ejecución condicional en virtud del intercambio de mensajes, fotografías y videos de carácter íntimo mediante la aplicación de mensajería instantánea WhatsApp con una menor de 13 años.

ACCEDER

ARGENTINA

GROOMING.

NULIDAD DE REQUERIMIENTO DE ELEVACIÓN A JUICIO.

IMPUTACIÓN.

PRINCIPIO DE CONGRUENCIA.

CÁMARA DE APELACIONES EN LO PENAL, PENAL JUVENIL, CONTRAVENCIONAL Y DE FALTAS SALA III - EXPTE. N° 41459/2019-5 - "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGÍAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL" - 28/09/2022.

Se rechazó -por mayoría- un planteo de nulidad del requerimiento de elevación a juicio interpuesto por la defensa del imputado por entender que no hubo afectación al principio de congruencia. Según la resolución, los actos procesales atacados consignaron y mantuvieron una plataforma fáctica y jurídica de la imputación lo suficientemente clara como para que el acusado conozca el suceso endilgado, y pueda, por tanto, ejercer sus derechos de manera eficiente.

ACCEDER

ARGENTINA

GROOMING.

CIBERACOSO.

JUICIO ABREVIADO.

JUZGADO DE CONTROL DE LA SEGUNDA CIRCUNSCRIPCIÓN JUDICIAL DE LA PROVINCIA DE LA PAMPA - EXPTE. N° 71369 - "MINISTERIO PÚBLICO FISCAL C/ A. A. A. S/ ABUSO SEXUAL SIMPLE - CIBERACOSO (DAM. Q. L.)" - 25/10/2022.

Se condenó a A.A.A. a una pena de 6 meses de prisión en suspenso por considerarlo responsable del delito de grooming. Se tuvo por acreditado el contacto del imputado con una menor de 13 años mediante la aplicación de mensajería instantánea WhatsApp donde se mantuvieron conversaciones con contenido sexual explícito.

ACCEDER

ARGENTINA

PRODUCCIÓN DE MATERIAL DE ABUSO SEXUAL INFANTIL.

ART. 128 CP.

CÁMARA DE APELACIONES EN LO PPJCYF - SALA II - EXPTE. N° CUIJ: DEB J-01-00014269-3/2019-2 - "B., M. G. SOBRE 92 - AGRAVANTES (CONDUCTAS DESCRIPTAS EN LOS ARTÍCULOS 89 /90 Y 91) " - 04/11/2022.

Se confirma la sentencia de primera instancia que condenó a M. G. B., por hallarlo autor penalmente responsable y a título de dolo del delito de producir material de abuso sexual infantil y de lesiones graves. Uno de los argumentos atacados por el imputado fue que su conducta era atípica. Frente a ello, la decisión analizó las características del tipo penal del art. 128 del CP y puntualizó que: "la norma citada prevé la producción por cualquier medio de toda representación de las partes genitales del menor con fines predominantemente sexuales".

ACCEDER

ARGENTINA

ABUSO SEXUAL.

EXPLOTACIÓN SEXUAL INFANTIL.

PRODUCCIÓN DE MATERIAL DE ABUSO SEXUAL INFANTIL.

TRIBUNAL ORAL EN LO CRIMINAL Y CORRECCIONAL N° 5 DE LA CAPITAL FEDERAL EXPTE. N° CCC 33955/2017/TO1 - 25/11/2022.

Se condenó a H.D.G. a una pena de 16 años y 6 meses por considerarlo autor de los delitos de producción y distribución de material de abuso sexual infantil reiterado en 39 oportunidades y de los delitos de abuso sexual agravado por haber sido cometido con acceso carnal, en concurso real con abuso sexual gravemente ultrajante, ambos calificados por ser el padre de la víctima, en concurso ideal con los delitos de promoción de la corrupción de menores agravado por tratarse del progenitor de la víctima. Las maniobras desplegadas se materializaron mediante la utilización de diversos soportes informáticos y redes sociales.

ACCEDER

VIOLENCIA DIGITAL

ARGENTINA

VIOLENCIA DE GÉNERO DIGITAL.

DIFUSIÓN NO CONSENTIDA DE IMÁGENES ÍNTIMAS.

"CÁMARA NACIONAL EN LO CIVIL, SALA M - EXPTE. N° 33626/2022 - "Q.C.E.S." C/ T.B. S/ DENUNCIA POR VIOLENCIA FAMILIAR" - 15/07/2022.

Q.C. denunció a su ex novio T.B. por violencia física, psicológica y por difundir videos íntimos manteniendo relaciones sexuales sin su consentimiento. La actora apeló la resolución de fecha 16/05/2022, con el fin de que el demandado borre todos los videos de su teléfono celular. Por decisión unánime se modificó dicha resolución y se le ordenó la eliminación de todo el material íntimo que tuviera en su dispositivo móvil como así también en la nube sin que quede almacenado en ningún tipo de sistema o soporte, en un plazo de 48 horas desde la notificación bajo apercibimiento de aplicar una multa de $1.000.000 ante su incumplimiento.

ACCEDER

ESPAÑA

RECURSO DE CASACIÓN DE LA ACUSACIÓN PARTICULAR ANTE EL TRIBUNAL SUPERIOR.

DELITO DE REVELACIÓN DE SECRETOS Y VEJACIONES LEVES.

TRIBUNAL SUPREMO, SALA DE LO PENAL - STS 699/2022 - 11/07/2022.

El Juzgado penal condenó al acusado por el delito de revelación de secretos (art. 197.7.2 del CP.) La Audiencia provincial de Oviedo revocó dicha condena por entender que, cuando el desnudo es parcial, porque la imagen solo capta el pecho, los hechos no tienen la suficiente gravedad para integrar el tipo penal.

El Tribunal Superior entiende que, aunque el desnudo sea solamente del torso, y no de cuerpo entero, se ve comprometido el bien jurídico protegido que es el ataque contra la intimidad de la denunciante, motivo por el que se casa y anula la sentencia de la audiencia provincial de Oviedo.

ACCEDER

ESPAÑA

RECURSO DE CASACIÓN DE LA DEFENSA ANTE EL TRIBUNAL SUPERIOR.

ACCESO A BASES DE DATOS PARA OBTENER INFORMACIÓN PERSONAL DE EX PAREJA.

TRIBUNAL SUPREMO, SALA DE LO PENAL - STS 3233/2022 - 21/07/2022.

El TS absolvió al acusado del delito de descubrimiento y revelación de secretos al que había sido condenado por entender que del relato de hechos probados nada se indicó sobre lo encontrado por el acusado en dichas bases, ni sobre la naturaleza sensible o sobre las consecuencias que se derivaron del conocimiento que se alcanzó, no concurriendo los elementos para subsumir la conducta en el tipo penal.

Se consideró que para condenar por el delito del art. 198 con relación al 197.2 CP es necesario que surja del relato de hechos probados en la sentencia la información que obtiene cuando se accede a una base de datos personales, como el detalle de las consecuencias derivadas de dicho conocimiento. Aplicándose el tipo penal si, en aquellos casos de acceso a la información (exceptuando datos sensibles), además se ocasionó un perjuicio al titular de los datos.

ACCEDER

COLOMBIA

ACCIÓN DE TUTELA.

DIFUSIÓN NO CONSENTIDA DE IMÁGENES ÍNTIMAS.

"REVISIÓN DE TUTELAS DE LA CORTE CONSTITUCIONAL DE COLOMBIA, SALA OCTAVA - SENTENCIA T-280/22 - 08/08/2022".

La accionante fue filmada sin que ella se diera cuenta en un baño del Centro de Equitación donde practicaba dicha actividad. En el video se muestran imágenes de sus zonas genitales y glúteos. En dicho caso, la Sala 8° solicitó se borre la filmación a los fines de la protección de la intimidad de la mujer y, por otro lado, exhortó al Congreso que promulgue nuevas leyes y medidas que prohíban las formas incipientes de violencia en razón de género en línea, el que abarca abusos que incluyen distribución no consensuada de contenido íntimo.

ACCEDER

ARGENTINA

VIOLENCIA DE GÉNERO DIGITAL.

UTILIZACIÓN DE IMÁGENES SIN CONSENTIMIENTO.

ACCIÓN PREVENTIVA DE DAÑOS.

"JUZGADO CIVIL Y COMERCIAL FEDERAL N° 7 - EXPTE. N° 4684/2020 - "MARZOL, NOELIA C/ GOOGLE INC. ACCIÓN PREVENTIVA DE DAÑOS" - 31/08/2022[2].

Se hizo lugar a una acción preventiva de daños interpuesta por Noelia Marzol contra Google Inc., en la cual la actora le solicita que elimine y bloquee las vinculaciones de su nombre y apellido con los sitios web pornográficos y sexuales en los cuales se exhibe un video que forma parte de su obra teatral llamada "SEX". La actora manifiesta que el video es un hecho de ficción indexado de su obra teatral en contra de su voluntad y sin su consentimiento, al cual se accede por intermedio del buscador de Google. Que la utilización sin consentimiento de su imagen no sólo afecta derechos de rango constitucional, además, constituye una modalidad de violencia de género que la ley 26.485 y los demás instrumentos internacionales pretenden erradicar. Se resuelve hacer lugar a la acción preventiva de daños.

ACCEDER

[2] Sobre este tema, ver también: https://ocedic.com/violencia-de-genero-en-la-web/

ARGENTINA

MOTORES DE BÚSQUEDA.
DAÑOS Y PERJUICIOS.
INDEMNIZACIÓN.

CÁMARA CIVIL Y COMERCIAL FEDERAL SALA III - EXPTE. N° 84756/2014/CA1 - "SABLICH MARÍA CELESTE ITATÍ C/ GOOGLE INC. Y OTROS S/ DAÑOS Y PERJUICIOS" - 15/11/2022.

Se resolvió hacer lugar a rubro indemnizatorio contra Google Inc. y Yahoo Argentina SRL por el daño causado a la actora por aparecer vinculación entre el nombre de la afectada y sitios pornográficos en los motores de búsqueda de las demandadas.

ACCEDER

ARGENTINA

VIOLENCIA DE GÉNERO.
AMENAZAS COACTIVAS.
UTILIZACIÓN DE MEDIOS ELECTRÓNICOS Y REDES SOCIALES.

CÁMARA NACIONAL DE CASACIÓN EN LO CRIMINAL Y CORRECCIONAL SALA 1 - EXPTE. N° CCC 12993/2016/TO3/CNC1 - "R., M. A. P. S/ RECURSO DE CASACIÓN" - 25/11/2022.

Se confirmó sentencia de Tribunal Oral que condenó a M.A.P.R. por considerarlo autor de amenazas coactivas llevadas a cabo en un contexto de violencia de género. La defensa particular del imputado había cuestionado, entre otros, la valoración probatoria del testimonio único de la damnificada y la existencia de la violencia de género.

ACCEDER

INTELIGENCIA ARTIFICIAL Y HERRAMIENTAS DISRUPTIVAS DE INVESTIGACIÓN EN EL DERECHO PENAL Y PROCESAL PENAL

ARGENTINA

PLANTEO DE NULIDAD.
ALLANAMIENTO.
AUTOINCRIMINACIÓN.
DISPOSITIVO TELEFÓNICO.
PATRÓN DE DESBLOQUEO.
APELACIÓN DE LA DEFENSA.

CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL SALA 5 - EXPTE. N° CCC 50979/2021/2/CA3 - "M. P. R. D. S/ NULIDAD" - 21/06/2022.

En un allanamiento derivado de un hecho de abuso se secuestró teléfono celular del imputado -medida que fue notificada a la defensa oficial, y cuestionada posteriormente-. En ese mismo acto, se le solicitó el patrón de desbloqueo del dispositivo, el cual fue aportado voluntariamente. La resolución estableció que si el imputado comprendía el alcance de la medida dispuesta y que la requisitoria fue voluntaria, la defensa no podría alegar que fue compelido al efecto.

ACCEDER

ARGENTINA

PLANTEO DE NULIDAD.
MANIPULACIÓN INFORMÁTICA.
CADENA DE CUSTODIA.

CÁMARA FEDERAL DE LA PLATA SALA III - EXPTE. N° FLP 20112/2020/9/CA5 - "PÉREZ BELLANDI, NELSON OSCAR S/ INCIDENTE DE NULIDAD" - 04/07/2022.

Nulidad planteada por la defensa del imputado por entender que fue violada la cadena de custodia de ciertos dispositivos peritados. La Sala III de la Cámara Federal de La Plata concluyó que no se vislumbró la presencia de vicio alguno que permitiera avanzar en la hipótesis defensista que argumentó la presencia de irregularidades y manipulación de la prueba en concreto.

ACCEDER

ARGENTINA

MEDIDA DE PRUEBA.

PLANTEO DE NULIDAD.

CADENA DE CUSTODIA.

COPIA FORENSE.

CÁMARA CRIMINAL Y CORRECCIONAL FEDERAL SALA I - EXPTE. N° CFP 1673/2013/24/-CA10 - "D., N. Y OTRO S/ INCIDENTE DE NULIDAD" - 19/08/2022.

Se confirmó rechazo de planteo de nulidad presentado por defensa técnica del imputado respecto de copia forense solicitada por la parte querellante AFIP por entender que se encontraba viciado el accionar de los peritos de Gendarmería Nacional. La resolución tuvo en consideración que la extracción y copia de la información contenida en los dispositivos incautados se trata de una medida de prueba tendiente al resguardo del material secuestrado y, de acuerdo al art. 233 del CPPN, en principio no requiere que el juez de intervención a las partes.

ACCEDER

ARGENTINA

SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS.

ACCIÓN DE AMPARO.

"JUZGADO EN LO CONTENCIOSO ADMINISTRATIVO Y TRIBUTARIO N° 4 DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE N° 182908/2020-0 - "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO O.D.I.A. Y OTROS C/ GCBA S/ AMPARO" - 07/09/2022.

El Observatorio de Derecho Informático Argentino (ODIA) interpuso acción de amparo contra la resolución 398/MJYSGC/19 que implementó el Sistema de Reconocimiento Facial de Prófugos sin encontrarse cumplidos los mecanismos normativos necesarios para garantizar el adecuado uso del sistema. Según el planteo, la principal falencia en dicho sistema conllevaría a que personas que se encuentren dentro del territorio de la Ciudad sean confundidas con prófugos de la justicia y detenidas por las fuerzas de seguridad, entre otras. La acción de amparo tuvo acogida favorable y el Juzgado en lo Contencioso Administrativo y Tributario Nro. 4 declaró la inconstitucionalidad de la Resolución en cuestión.

ACCEDER

ESPAÑA

RECURSO DE CASACIÓN DE LA DEFENSA ANTE EL TRIBUNAL SUPERIOR.

EVIDENCIA DIGITAL.

CONVERSACIONES DE *WHATSAPP.*

DICTAMEN PERICIAL DE AUTENTICIDAD.

TRIBUNAL SUPREMO, SALA DE LO PENAL - EXPTE. N° STS 3318/2022 - 22/09/2022.

La Audiencia provincial condenó al acusado como autor de varios delitos cometidos contra menores, entre ellos difusión de material de abuso sexual infantil. La sentencia condenatoria se basó, entre otras pruebas, en las conversaciones de WhatsApp aportadas por las víctimas. La defensa recurre en casación, alegando -entre otros motivos- falta de dictamen pericial de autenticidad de las conversaciones del acusado con los menores. El Tribunal Supremo entendió que en los casos que existan otros elementos de prueba que aseveren la comunicación y descarten cualquier tipo de duda sobre la autenticidad, no existe vulneración a la presunción de inocencia, aunque no exista dicho dictamen pericial.

ACCEDER

ARGENTINA

EVIDENCIA DIGITAL.

PERITAJE DISPOSITIVO TELEFÓNICO.

JUZGADO DE CONTROL N° 3 DE JUJUY - EXPTE. N° P-265002-MPA/22 - "ARANCIBIA NICOLÁS MAXIMILIANO P.S.A. ESTAFA - CIUDAD" - 03/10/2022.

Se hizo lugar a la extracción de datos digitales de un teléfono celular perteneciente a una persona imputada de estafa al considerar debidamente fundada la petición del Agente Fiscal de la Unidad Fiscal de Delitos Patrimoniales. Se argumentó que del análisis informático de los archivos extraídos de los bienes cautelados se podría obtener prueba de relevancia para el esclarecimiento del hecho investigado, resultando suficiente la orden judicial con el objeto de no vulnerar garantías amparadas constitucionalmente.

ACCEDER

ESPAÑA

RECURSO DE CASACIÓN DE LA DEFENSA ANTE EL TRIBUNAL SUPERIOR.

INFORMACIÓN OBTENIDA DE GPS SIN AUTORIZACIÓN JUDICIAL.

TRIBUNAL SUPREMO, SALA DE LO PENAL - STS 3777/2022 - 21/10/2022.

En este caso, tal como lo entendió la Audiencia Provincial, los agentes policiales no instalaron ningún dispositivo de seguimiento del vehículo del acusado. En efecto, al tratarse de un coche de alquiler con dispositivo GPS ya instalado, el solicitar los datos a la empresa se considera una diligencia de investigación proporcional y necesaria, siendo que los datos obtenidos solo muestran posición del vehículo en un período de tiempo breve, sin aportar datos de sonido o imagen. El TS concluye que los datos obtenidos por los agentes no comprometen el derecho al secreto de las comunicaciones, ni el derecho a la intimidad, no siendo necesaria la previa autorización judicial. Por lo anteriormente expuesto, el TS desestima el motivo del recurso.

ACCEDER

FRANCIA

AUTOINCRIMINACIÓN.

DISPOSITIVO TELEFÓNICO.

PATRÓN DE DESBLOQUEO.

TRIBUNAL DE CASACIÓN - ASAMBLEA PLENARIA (FRANCIA) - RECURSO N° 21-83.146 - 07/11/2022.

La Asamblea Plenaria intervino en un caso donde un imputado se negó a comunicar a los investigadores la contraseña para desbloquear dos dispositivos telefónicos encontrados en su automóvil y que fueran utilizados en un contexto de tráfico de drogas. El cuestionamiento planteado se circunscribió a definir si el código para desbloquear la pantalla de inicio de un teléfono es o no una "convención secreta para descifrar un medio de criptografía", en el sentido de la ley penal francesa. Frente a ello, se estableció que si el dispositivo telefónico está equipado con un "medio de criptografía", el código de desbloqueo de su pantalla de inicio puede constituir una "clave de descifrado". En ese caso, el titular del teléfono, siendo informado de las consecuencias penales de un rechazo, está obligado a dar a las autoridades el código de desbloqueo de la pantalla de inicio. Si se niega a comunicar esa clave, comete la infracción de "negarse a entregar una convención secreta de descifrado de un medio de criptología susceptible de haber sido utilizado para preparar, facilitar o cometer un crimen o delito".

ACCEDER

ARGENTINA

PRUEBA ANTICIPADA.

REDES SOCIALES.

IDENTIDAD DIGITAL.

CÁMARA CIVIL SALA J - EXPTE. N° 11164/2021 - "A, I.A. C/ RESPONSABLE DE LOS HECHOS OCURRIDOS EL 21 Y 22 DE AGOSTO DE 2017 Y OTRO S/ PRUEBA ANTICIPADA" - 17/11/2022.

Se admitieron parcialmente agravios de la parte actora en un requerimiento de prueba anticipada contra Facebook Argentina (Meta Platforms Inc.), y se dispuso se reitere oficio a la citada empresa a los efectos de que arbitre los medios necesarios para obtener información sobre titulares de cuentas de las plataformas denunciadas por el uso indebido de una identidad digital ajena.

ACCEDER

ATAQUES INFORMÁTICOS Y FRAUDE

ARGENTINA

JUICIO ABREVIADO.

CONDENA.

DEFRAUDACIÓN MEDIANTE TÉCNICAS DE MANIPULACIÓN INFORMÁTICA.

TRIBUNAL ORAL EN LO CRIMINAL Y CORRECCIONAL N° 3 DE LA CAPITAL FEDERAL - EXPTE. CCC 36928/2016/TO1 - REG. INT. N° 5965 Y 6040 - 01/07/2022.

En juicio abreviado se condenó a dos personas por haber efectuado numerosas transferencias electrónicas desde cuentas bancarias ajenas hacia las de los imputados -operaciones que fueron desconocidas por los titulares y que tampoco pudieron ser justificadas por los involucrados-.

ACCEDER

ARGENTINA

VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD.

VIOLENCIA DE GÉNERO DIGITAL.

DELITO DE ACCIÓN PÚBLICA.

CÁMARA DE APELACIONES EN LO PENAL, PENAL JUVENIL, CONTRAVENCIONAL Y DE FALTAS SALA I - EXPTE. N° 1756290/2022 - "C, G.A. S/ 153 BIS - ACCESO SIN AUTORIZACIÓN A UN SISTEMA O DATO INFORMÁTICO DE ACCESO RESTRINGIDO" - 04/07/2022.

Se denuncia el ingreso sin autorización, por parte de G. A. C., al Instagram y Facebook, pertenecientes a su ex pareja, y modificar la contraseña de acceso a las cuentas de las referidas redes sociales, impidiendo el acceso a su titular. La defensa plantea una excepción de falta de acción, sosteniendo que el art. 153 bis es un delito de acción privada. La Fiscalía señaló que el delito del art. 153 bis del CP queda alcanzado para los delitos de acción pública y que corresponde la intervención del MPF ya que el caso se encuentra enmarcado en un contexto de violencia de género.
El Tribunal confirma la resolución que no hace lugar al planteo de falta de acción, por entender que las conductas investigadas en el presente proceso, conforme la habilitación punitiva del art. 153 bis CP, no constituyen violación de secretos, sino accesos no autorizados a distintas redes sociales. La acción investigada no puede considerarse comprendida en el art. 73 inciso 2° CP, por cuanto no se trata de "violación de secretos", sino, como "violación de la privacidad", regida por el régimen general previsto en el art. 71 CP: acción penal pública.

ACCEDER

ARGENTINA

SUSPENSIÓN DE JUICIO A PRUEBA.

DEFRAUDACIÓN MEDIANTE TÉCNICAS DE MANIPULACIÓN INFORMÁTICA.

JUZGADO EN LO PENAL, CONTRAVENCIONAL Y DE FALTAS N° 8 DE LA CIUDAD DE BUENOS AIRES - EXPTE. N° 26836/2022 - "P.G.H.E Y OTROS S/INF. ART. 173, INCISO 16 DEL C.P" - 15/07/2022.

Acuerdo entre el Ministerio Público Fiscal y la Defensa Particular en donde se dispuso la suspensión del juicio a prueba respecto de dos personas que se encontraban imputadas del delito tipificado por el art. 173 inc. 16 CP (audiencia conf. art. 278 del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires).

ACCEDER

ARGENTINA

FALTA DE MÉRITO.

DEFRAUDACIÓN MEDIANTE UTILIZACIÓN DE TARJETA DE CRÉDITO.

SUSTRACCIÓN DE DATOS.

JUZGADO DE CONTROL N° 2 DE SAN SALVADOR DE JUJUY. EXPTE. N° P-259863-MPA/21 - "CRAUZAS, GISSEL IVANA P.S.A. DEFRAUDACIÓN CON TARJETA DE COMPRA, CRÉDITO O DÉBITO - CIUDAD" - 09/08/2022.

Se resolvió no hacer lugar al requerimiento de elevación a juicio impulsado por el Ministerio Público Fiscal y se declaró la falta de mérito contra G. I. C. a quien se le imputó haber obtenido los datos de la tarjeta de crédito del Banco BBVA Visa del Sr. V. L. G. y abusando de la confianza, haber utilizado dichos datos de forma no autorizada a los efectos de efectuar compras virtuales de prendas de niños ocasionando un perjuicio patrimonial a la víctima.

ACCEDER

ARGENTINA

CRIPTOACTIVOS.

INMOVILIZACIÓN DE CUENTA.

JUZGADO NACIONAL EN LO CRIMINAL Y CORRECCIONAL N° 18 - 17/08/2022.

Se dispuso la entrega de criptoactivos oportunamente inmovilizados en la cuenta de un imputado en la plataforma "Binance", en favor de la víctima que sufrió el robo de su celular y posteriormente la sustracción de aquel dinero virtual. La entrega se efectivizó en carácter de depositario judicial, con la expresa prohibición de poder utilizarlos hasta tanto se descarte su eventual afectación en los términos de los arts. 23 del CP y 523, último párrafo, del CPPN.

ACCEDER

ARGENTINA

AUDIENCIA DE CONCILIACIÓN.

ROBO SIMPLE. CONCURSO. ART. 173 INC. 16 CP.

TRIBUNAL ORAL EN LO CRIMINAL Y CORRECCIONAL N° 3 DE LA CAPITAL FEDERAL - EXPTE. N° CCC 18911/2022/TO1 - 20/09/2022.

Se resolvió dictar la extinción de la acción penal y el pronunciamiento de sobreseimiento de C. E. G. R., en orden al delito de robo simple en concurso real con defraudación mediante manipulación informática en virtud de haberse acreditado la condición fijada en el acuerdo conciliatorio arribado entre la parte damnificada y el imputado a través del pago de $140.000.

ACCEDER

ARGENTINA

DESESTIMACIÓN DE DENUNCIA POR PARTE DEL MPF.

ESTAFA.

NULIDAD DE DICTAMEN FISCAL.

CÁMARA NACIONAL DE CASACIÓN EN LO CRIMINAL Y CORRECCIONAL SALA DE TURNO EXPTE. N° CCC8822/2022/1/RH1 - 21/09/2022.

Se rechazó recurso de queja interpuesto por el representante del Ministerio Público Fiscal por medio del cual se intentó continuar con la decisión de desestimar denuncia por estafa interpuesta por la damnificada A.B.P. El dictamen de la fiscalía había concluido que en el caso bajo estudio no se había verificado la utilización de un ardid o un engaño con idoneidad y significancia jurídica a partir del cual se haya hecho incurrir al sujeto pasivo en un error, sino que había operado una falta total de diligencia de su parte.

ACCEDER

En sentido similar: **CONSULTAR**

RESPONSABILIDAD DE LAS ENTIDADES BANCARIAS

ARGENTINA

RESPONSABILIDAD BANCARIA.

NULIDAD.

ESTAFA ELECTRÓNICA.

JUZGADO NACIONAL DE 1° INSTANCIA EN LO COMERCIAL N° 10 - EXPTE. N° 331/2021 - "GABRIELICH, SILVIA ELIANA C/ BANCO SANTANDER RÍO S.A. S/ ORDINARIO" - 07/07/2022.

Se hizo lugar a la demanda por daños y se condenó al Banco Santander Río S.A. a efectuar el reintegro de los montos sustraídos o debitados antijurídicamente de la cuenta de la parte actora en ocasión del fraude electrónico sufrido. Asimismo, la entidad bancaria deberá abonar un resarcimiento por daño moral y la multa civil por daño punitivo y costas. En la decisión se evaluó si resultaba procedente imputar responsabilidad al Banco Santander Río S.A. o se debía tener a la actora como responsable de las consecuencias derivadas de su actuar negligente.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.

NULIDAD.

ESTAFA ELECTRÓNICA.

CÁMARA CIVIL Y COMERCIAL COMÚN DE CONCEPCIÓN DE TUCUMÁN SALA II - EXPTE. N° 9/21 - "G. J. E. C/ BANCO MACRO SA S/ DAÑOS Y PERJUICIOS" - 29/07/2022.

Se rechazó planteo de una entidad bancaria contra sentencia que declaró nulidad de préstamos preaprobados que no fueran realmente solicitados por un cliente y se la condenó al pago de sumas de dinero en concepto de daño moral y daño punitivo. Se entendió que el banco involucrado incumplió las obligaciones de seguridad que derivan de la relación de consumo, deberes que imponen a la entidad extremar las medidas con el objeto de evitar los reiterados ataques y fraudes informáticos que se suscitan a través del uso de nuevas tecnologías.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.
NULIDAD.
ESTAFA ELECTRÓNICA.

JUZGADO COMERCIAL N° 57 SECRETARÍA N° 54 - EXPTE. N° 13927/2020 - "F.M.L. C/ BANCO BBVA ARGENTINA S.A. S/ SUMARÍSIMO" - 01/08/2022.

Se hizo lugar a demanda sumarísima promovida contra el Banco BBVA Argentina S.A., se declaró nulidad de préstamo preaprobado gestionado por terceras personas en la cuenta bancaria de la actora y se impuso el pago de sumas de dinero en concepto de daño moral y punitivo.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.
FALLA DE SEGURIDAD.
TARJETAS DE CRÉDITO.

CÁMARA NACIONAL DE APELACIONES EN LO COMERCIAL SALA D - EXPTE. N° 13.008/2018 - "PISATURO, DAMIÁN HUGO C/ INDUSTRIAL AND COMMERCIAL BANK OF CHINA (ARGENTINA) S.A. Y OTRO S/ ORDINARIO" - 01/09/2022.

Se confirmó sentencia de primera instancia que condenó solidariamente al banco ICBC Argentina S.A. y First Data Cono Sur S.R.L. al pago de sumas de dinero en concepto de devolución de cargos efectuados a la actora como consecuencia de extracciones dinerarias efectuadas por terceros, daño moral e intereses, por considerarlas responsables por la falla de seguridad del servicio prestado a través de terminales electrónicas de operaciones bancarias.

ACCEDER

ARGENTINA

VISHING.
REDES SOCIALES.
HOMEBANKING.

JUZGADO CIVIL, COMERCIAL, MINERÍA Y SUCESIONES N° 3 (UNIDAD JURISDICCIONAL 3), VIEDMA, PROVINCIA DE RÍO NEGRO - EXPTE. N° B-1VI-511-C2020 - "ELORZA FERNÁNDEZ, MARÍA ROMINA C/ BANCO PATAGONIA S/ DAÑOS Y PERJUICIOS (SUMARÍSIMO)" - 07/09/2022.

Se hizo lugar a una demanda de daños y perjuicios contra el Banco Patagonia S.A. por un contrato de mutuo preaprobado generado fraudulentamente a través de la cuenta de homebanking de la actora y se declaró su nulidad. La resolución advirtió el deficiente control ejercido por la entidad financiera para impedir la efectivización de la maniobra delictiva concluyendo que las medidas de seguridad utilizadas por la demandada no resultaron eficaces para evitarla.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.
NULIDAD.
ESTAFA ELECTRÓNICA.

JUZGADO CIVIL Y COMERCIAL N° 25 DE LA PLATA - EXPTE. N° LP - 41853/2020 - "BALVERDI, LUCIANO GERARDO C/ BANCO DE LA PROVINCIA DE BUENOS AIRES" S/ NULIDAD DE CONTRATO (DIGITAL)" - 19/09/2022.

Se hizo lugar a una demanda de nulidad de contrato y daños y perjuicios contra el Banco de la Provincia de Buenos Aires vinculado a un préstamo preaprobado generado por terceras personas en la cuenta bancaria de la accionante. La resolución tuvo en cuenta que el sistema informático utilizado por la demandada permitía en el lapso de 24 horas obtener una clave, contraer préstamos, transferir a cuentas no vinculadas y con las que antes no se efectuaron transacciones, requerir un adelanto de haberes y todo por sumas importantes de dinero, sin las medidas de seguridad esperables y que garanticen un vínculo de confianza con sus clientes.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.
NULIDAD.
ESTAFA ELECTRÓNICA.

CÁMARA DE APELACIONES EN LO CIVIL, COMERCIAL, FAMILIA Y MINERÍA 1°, VIEDMA - EXPTE. N° VI-31306-C-0000 - "BARTORELLI, EMMA GRACIELA C/ BANCO PATAGONIA S.A. S/ DAÑOS Y PERJUICIOS (SUMARÍSIMO)" - 29/09/2022.

Se resolvió rechazar un recurso de apelación interpuesto por el Banco Patagonia S.A. contra la sentencia de primera instancia que hizo lugar a una demanda de daños y perjuicios, declaró la nulidad de un préstamo gestionado por terceras personas a través de Homebanking, y condenó a la entidad bancaria al pago de un resarcimiento económico. La decisión concluyó que la damnificada no actuó de manera negligente, sino que "determinadas debilidades del sistema bancario, hoy en día bastante mejorado, posibilitaron que la actora y muchos miles más, todos los días sean víctimas de estos estafadores" sumado a un deficiente control ejercido por la entidad financiera para impedir la efectivización de la maniobra delictiva en cuestión.

ACCEDER

ARGENTINA

MULTA.
ENTIDAD BANCARIA.
CONSUMIDORES.

CÁMARA CONTENCIOSO ADMINISTRATIVO FEDERAL SALA IV - EXPTE. N° 19719/2021 - "BANCO SANTANDER RÍO S.A. C/ EN-M DESARROLLO PRODUCTIVO (EX 3316571/21 - DISP 452/21) S/ RECURSO DIRECTO LEY 24.240 - ART. 45" - 04/10/2022.

Se rechazó recurso de apelación interpuesto por el Banco Santander Río S.A. contra la Disposición 452/21 por medio de la cual el Director Nacional de Defensa del Consumidor y Arbitraje del Consumo impuso a la referida entidad bancaria una multa de $5.000.000, por infracción a los arts. 4, 5, 8 bis y 19 de la Ley 24.240, por cuanto: i) no brindó información cierta, clara y detallada respecto de los riesgos existentes en la operatoria comercial a su cargo; ii) no cumplió con la obligación de seguridad del servicio brindado, en atención a que muchos consumidores fueron víctimas de diferentes métodos de estafas utilizando la tecnología ofrecida por el banco sumariado, posibilitando que terceros accedieran a las cuentas de clientes damnificados y así extrajeran dinero o pactaran créditos personales cuyos montos habrían sido transferidos a cuentas bancarias de terceros; iii) no garantizó condiciones de atención y trato digno y equitativo a los consumidores dado que, pese a que los damnificados iniciaron reclamos en sus correspondientes entidades bancarias, no recibieron respuesta adecuada ni una solución a sus problemas; y iv) no prestó el servicio de acuerdo a los términos, plazos, condiciones, modalidades, reservas y demás circunstancias conforme a las cuales fueron ofrecidos, publicitados o convenidos.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.

NULIDAD.

ESTAFA ELECTRÓNICA.

JUZGADO CIVIL, COMERCIAL, MINERÍA Y SUCESIONES N° 1, VIEDMA - EXPTE. N° VI-14379-C-0000 - "LINARES, MARCELA VALERIA C/ BANCO PATAGONIA S.A. S/ DAÑOS Y PERJUICIOS (SUMARÍSIMO)" - 02/11/2022.

Se declaró la nulidad de un contrato de préstamo generado a través de la plataforma de Homebanking del Banco Patagonia S.A. y se condenó a la entidad bancaria al pago de una suma resarcitoria y a la devolución de los montos debitados en concepto de cuotas. La decisión tuvo en cuenta que la entidad bancaria debió implementar como medida de seguridad un sistema de alerta -preventivo- frente a las transacciones virtuales ofrecidas en su web.

ACCEDER

ARGENTINA

RESPONSABILIDAD BANCARIA.

NULIDAD.

JUZGADO EN LO CIVIL Y COMERCIAL DE LA 1° NOMINACIÓN DE VENADO TUERTO, PROVINCIA DE SANTA FE - "DUFOUR, DANIELA NATALIA C/ BANCO HIPOTECARIO S.A. S/ MEDIDA CAUTELAR INNOVATIVA" - 09/11/2022.

Se hizo lugar a demanda que solicitó se declare la nulidad de préstamo bancario solicitado por terceras personas. La entidad bancaria vencida deberá reintegrar los montos debitados a la actora y abonar sumas de dinero correspondientes a daño moral y punitivo. Actualmente, la resolución se encuentra apelada por la parte demandada.

ACCEDER

MEDIDAS CAUTELARES VINCULADAS A ATAQUES INFORMÁTICOS

ARGENTINA

MEDIDA AUTOSATISFACTIVA.

FRAUDE INFORMÁTICO.

CÁMARA CIVIL Y COMERCIAL DE LA PROVINCIA DE FORMOSA - EXPTE. N° 12.551/22 - "NISSEN, MARÍA FERNANDA C/ BANCO DE FORMOSA S.A. S/ MEDIDA AUTOSATISFACTIVA" - 11/08/2022.

Se confirmó medida autosatisfactiva promovida por la Sra. M. F. N. contra el Banco de Formosa S.A., en virtud de la cual se condenó a la sociedad a restituir a la Sra. N. la suma de $100.000, quien habría sido víctima de una maniobra de fraude informático.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR.

ESTAFA ELECTRÓNICA.

JUZGADO CIVIL, COMERCIAL, MINERÍA Y SUCESIONES N° 9, GENERAL ROCA - EXPTE. N° RO-00539-C-2022 - "REGALÍA, JUAN MANUEL C/ CRÉDITOS AL RÍO S.A. S/ MEDIDA CAUTELAR (AUTÓNOMAS) - MEDIDA CAUTELAR" - 11/08/2022.

Se hizo lugar a medida cautelar innovativa contra la sociedad Créditos Al Río S.A. ordenando a la entidad crediticia se abstenga de realizar descuentos en cuentas de titularidad de la actora por un préstamo que no fuera por ella solicitado, como así también de realizar ejecuciones judiciales e intimaciones extrajudiciales; se suspenda el cómputo de intereses moratorios, compensatorios, punitorios, financieros, y la aplicación íntegra del contrato; y se proceda a informar al BCRA que la situación crediticia sería la correspondiente a la categoría N° 1, hasta tanto se resuelva sobre el fondo de la cuestión debatida en el proceso principal.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR.

ESTAFA ELECTRÓNICA.

CÁMARA FEDERAL DE LA PLATA SALA II - EXPTE. N° FLP 14868/2021/CA1 - "TROGLIA, SUSANA ELIDA C/ BANCO DE LA NACIÓN ARGENTINA S/ LEY DEL CONSUMIDOR" - 22/08/2022.

Se confirmó decisión que hizo lugar a una medida cautelar contra el Banco de la Nación Argentina, ordenado a dicha entidad se abstenga de efectuar descuentos sobre las cuentas bancarias de la parte actora en relación a supuestos préstamos o créditos que no fueran por ella contratados, y de efectuar acciones legales tendientes al cobro de las sumas involucradas en la maniobra denunciada. Uno de los fundamentos de la resolución destacó que el Banco Central de la República Argentina estableció la imposición a los bancos de contar con mecanismos de seguridad informática con la finalidad de garantizar la confiabilidad de la operatoria mediante canales electrónicos, obligación que debiera aparecer robustecida en el marco de una emergencia sanitaria.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR DE NO INNOVAR.

ESTAFA ELECTRÓNICA.

SUPLANTACIÓN DE IDENTIDAD.

JUZGADO DE FAMILIA, CIVIL, COMERCIAL, MINERÍA Y SUCESIONES N° 11, EL BOLSÓN - EXPTE. N° EB-00011-C-2022 - "CAPELLA, SILVINA PAOLA C/ MERCADO LIBRE S.R.L. S/ SUMARÍSIMO - NULIDAD, MEDIDA CAUTELAR, DAÑOS Y PERJUICIOS" - 08/09/2022.

Se hizo lugar a una medida cautelar de no innovar contra la empresa Mercado Libre ordenando a la empresa se abstenga de efectuar descuentos dinerarios vinculados a diferentes transacciones llevadas a cabo por terceras personas en nombre de la actora, originados como consecuencia de la sustracción de su teléfono móvil y posterior acceso indebido a la plataforma digital de Mercado Pago. Los argumentos que fundaron la medida se circunscribieron a la relación de consumo entre las partes y la correspondiente tutela preventiva de los consumidores.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR.

ENTIDAD BANCARIA.

ESTAFA ELECTRÓNICA.

CÁMARA SEGUNDA EN LO CIVIL Y COMERCIAL DE LA PLATA, SALA II - EXPTE. N° 132959-1 - "PARDO, SILVIA GRACIELA C/ BANCO DE LA PROVINCIA DE BUENOS AIRES S/ NULIDAD DE CONTRATO S/ INCIDENTE ART. 250 CPCC" - 11/10/2022.

Se confirmó medida cautelar innovativa solicitada por una persona damnificada por una maniobra de estafa electrónica y se ordenó al Banco de la Provincia de Buenos Aires la suspensión de descuentos y/o retenciones que hubiese correspondido practicar respecto de la actora sobre su cuenta bancaria como consecuencia de los préstamos solicitados por terceras personas. La decisión desechó los argumentos defensistas de la entidad bancaria que invocó la responsabilidad de la actora por brindar voluntariamente sus claves personales a terceros, y destacó que las medidas bancarias vigentes se tornaron obsoletas o insuficientes.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR.

ESTAFA ELECTRÓNICA.

CÁMARA NACIONAL DE APELACIONES EN LO CIVIL Y COMERCIAL FEDERAL SALA II - EXPTE. N° 12391/2022 - "LAGUILLÓN, SUSANA MARÍA C/ BANCO DE LA NACIÓN ARGENTINA S/ MEDIDAS CAUTELARES" - 13/10/2022.

Se revocó resolución de primera instancia que no hizo lugar a medida cautelar contra el Banco de la Nación Argentina tendiente a disponer la suspensión de pagos de cuotas derivadas de un préstamo personal solicitado por terceras personas a nombre de la parte actora mediante el servicio de Homebanking. Para así decidir, se analizó el compromiso que deben asumir las entidades bancarias para garantizar las medidas de seguridad necesarias a fin de evitar que ocurran maniobras defraudatorias y la especial relación entre las partes ante un contrato de consumo, donde la parte más débil resulta ser la usuaria de un sistema informático diseñado por el propio Banco involucrado.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR
DE NO INNOVAR.

ESTAFA ELECTRÓNICA.

JUZGADO NACIONAL EN LO COMERCIAL N° 31 SECRETARÍA N° 62 - EXPTE. N° 17.329/22- "T., R. B. L. C/ BANCO SUPERVIELLE S.A. S/MEDIDA PRECAUTORIA" - 24/10/2022.

Se hizo lugar a la medida de no innovar solicitada por la parte actora, ordenándose a la entidad bancaria que le restituya la suma de $184.098 correspondiente al saldo en pesos que tenía en sus cuentas. Dicha suma habría sido sustraída mediante una maniobra fraudulenta cometida por un tercero, quién habría utilizado una tarjeta SIM duplicada para acceder a los datos bancarios que se encontraban en el celular de la víctima. El fallo hace especial referencia a la asimetría con la que nacen las relaciones de consumo, agravado en materia de seguridad informática, recayendo sobre la entidad bancaria una obligación expresa de seguridad y garantía respecto de los usuarios con los que ha contratado.

ACCEDER

ARGENTINA

MEDIDA CAUTELAR.

ESTAFA ELECTRÓNICA.

SECRETARÍA DE CONSUMO N° 3 - OFICINA DE GESTIÓN JUDICIAL - EXPTE. N° 361158/2022-0 "A., J. CONTRA BANCO DE LA NACIÓN ARGENTINA S.A. SOBRE INCIDENTES - RC - MEDIDA CAUTELAR" - 30/11/2022.

Se hizo lugar a una medida cautelar contra el Banco de la Nación Argentina S.A. -en forma parcial- y se le ordenó arbitre los medios necesarios para proceder a la suspensión de cualquier débito en las cuentas bancarias de titularidad del Sr. A. J. por el cobro de las cuotas de un mutuo solicitado por terceras personas, hasta tanto se decida sobre el fondo de la cuestión o, en su caso, se cumpla el plazo previsto en el artículo 134 del CPJRC.

ACCEDER

COMPETENCIA EN MATERIA DE ATAQUES INFORMÁTICOS[3]

ARGENTINA

CONFLICTO DE COMPETENCIA ENTRE FUERO DE LA CIUDAD Y NACIONAL EN LO CRIMINAL Y CORRECCIONAL.

ART. 172 Y 173 INC. 16 CP.

APELACIÓN DEL MINISTERIO PÚBLICO FISCAL DE LA CIUDAD.

CÁMARA DE APELACIONES EN LO PENAL, PENAL JUVENIL, CONTRAVENCIONAL Y DE FALTAS, SALA III - EXPTE. N° 163855-2021-0 - "FIORI, GABRIEL RICARDO" - 30/06/2022.

Se confirmó resolución de primera instancia donde se decidió que los hechos denunciados eran subsumibles en el tipo penal previsto en el delito de estafa (art. 172 CP) y por tanto debían ser juzgados por el fuero nacional. La resolución concluyó que ninguna de las operaciones desplegadas contenidas en la maniobra generaron una alteración del normal funcionamiento del sistema informático involucrado en los términos requeridos por el tipo penal de defraudación informática, delito que sí resultaría ser de competencia de la Ciudad.

ACCEDER

ARGENTINA

CONFLICTO DE COMPETENCIA TERRITORIAL ENTRE FUERO FEDERAL CONCORDIA Y NACIONAL.

FRAUDES INFORMÁTICOS.

CÁMARA CRIMINAL Y CORRECCIONAL FEDERAL SALA I - EXPTE. N° CFP 7148/20/44/CA10 - "A., L. Y OTRO S/ COMPETENCIA" - 02/08/2022.

Se confirmó rechazo de declinatoria de competencia ante la imposibilidad de escindir hechos que se produjeron en diferentes ámbitos territoriales. Para ello, se tuvo en cuenta que la maniobra investigada está compuesta por una estructura ilícita compleja que supera ampliamente los hechos delictivos que tuvieron lugar en la ciudad de Entre Ríos.

ACCEDER

ARGENTINA

CONFLICTO DE COMPETENCIA ENTRE FUERO DE LA CIUDAD Y NACIONA EN LO CRIMINAL Y CORRECCIONAL.

ART. 172 CP.

REDES SOCIALES.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 203098/2021-1 - "INCIDENTE DE INCOMPETENCIA EN AUTOS "NN, NN SOBRE 173. 16 - ESTAFA INFORMÁTICA"" - 17/08/2022.

Se resolvió declarar la competencia del Juzgado Nacional en lo Criminal y Correccional N° 62, en virtud de que el hecho investigado encuadraría preliminarmente en el art. 172 del CP.

ACCEDER

En similar sentido, consultar: **ANEXO N° 1**[4]

[3] Ver también doctrina vinculada en este número: "Ciberestafas: Conflictos de competencia en la Ciudad de Buenos Aires".

[4] Si bien en estos fallos las maniobras defraudatorias son distintas, todas ellas fueron encuadradas en el art. 172 del CP y se declaró la competencia de la Justicia Nacional en lo Criminal y Correccional.

ARGENTINA

CONFLICTO DE COMPETENCIA ENTRE FUERO DE LA CIUDAD Y NACIONAL EN LO CRIMINAL Y CORRECCIONAL.

ART. 173 INC. 16 CP.

HOMEBANKING.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD DE BUENOS AIRES - EXPTE. N° TSJ 140554/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS "NN, NN SOBRE 173 INC. 15 S/ CONFLICTO DE COMPETENCIA"" - 24/08/2022.

Se resolvió declarar la competencia del Juzgado en lo Penal, Contravencional y de Faltas N°2, en virtud de que el hecho investigado encuadraría preliminarmente en el art. 173 inc. 16 del CP.

ACCEDER

En similar sentido:

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD DE BUENOS AIRES - EXPTE. N° INC 26089/2022-1 - "INCIDENTE DE INCOMPETENCIA EN AUTOS "NN, NN SOBRE 173. 16 S/ ESTAFA INFORMÁTICA"" - 03/08/2022.

CONSULTAR

CÁMARA DE APELACIONES EN LO PENAL, PENAL JUVENIL, CONTRAVENCIONAL Y DE FALTAS SALA III - EXPTE. N° IPP 225985/2021-0 - "PIANOVI, GUSTAVO FABIÁN SOBRE 172 - ESTAFA" - 12/08/2022.

CONSULTAR

ARGENTINA

CONFLICTO DE COMPETENCIA ENTRE FUERO CIVIL Y COMERCIAL FEDERAL Y JUZGADO FEDERAL DE QUILMES.

DAÑOS DERIVADOS DE UN FRAUDE INFORMÁTICO.

CÁMARA CIVIL Y COMERCIAL FEDERAL SALA III - EXPTE. N° CCF 11.130/2021/CA1 - "VINCHI, LEONARDO GABRIEL C/ BANCO DE LA NACIÓN ARGENTINA S/ RESPONSABILIDAD POR DAÑOS" - 08/11/2022.

Se resolvió declarar la competencia del Juzgado Nacional en lo Civil y Comercial Federal N°6, en razón del art. 1° del Código Procesal Civil y Comercial que dispone que la competencia territorial en cuestiones patrimoniales es esencialmente prorrogable entre las partes.

ACCEDER

ARGENTINA

CONFLICTO DE COMPETENCIA ENTRE FUERO DE LA CIUDAD Y NACIONAL EN LO CRIMINAL Y CORRECCIONAL.

ART. 173 INC. 16 CP.

CÁMARA NACIONAL DE CASACIÓN EN LO CRIMINAL Y CORRECCIONAL SALA 2 - EXPTE. N° CCC 7337/2021/TO1/CNC1 - 11/11/2022.

Se resolvió declarar la competencia del Tribunal Oral en lo Criminal y Correccional N°16. Se advirtió que el hecho investigado corresponde a un tipo penal creado con posterioridad a la ley 24.588 (art. 173 inc. 16 del CP) donde no está prevista la transferencia de competencia respecto del delito de defraudación informática.

ACCEDER

JURISPRUDENCIA

ANEXO Nº 1

COMPETENCIA EN MATERIA DE ATAQUES INFORMÁTICOS

El presente tiene como finalidad completar el listado de fallos relacionados con conflictos de competencia, tratándose de casos en los que las distintas maniobras defraudatorias fueron encuadradas en el art. 172 del CP y se declaró la competencia de la Justicia Nacional en lo Criminal y Correccional[1].

ARGENTINA

PUBLICACIÓN ENGAÑOSA ZONAPROP.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 4309/2022-1 - "INCIDENTE DE INCOMPETENCIA EN AUTOS "NN, NN SOBRE 172 - ESTAFA"" - 13/07/2022.

ACCEDER

VENTA DE MONEDA EXTRANJERA. SUPLANTACIÓN DE IDENTIDAD.

WHATSAPP.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 247276/2021-1 - "INCIDENTE DE INCOMPETENCIA EN AUTOS "NN, NN SOBRE 71 QUINQUIES 1ER PÁRR - SUPLANTACIÓN DE IDENTIDAD" - 03/08/2022.

ACCEDER

VENTA DE BIENES.

INSTAGRAM.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 235196/2021-1- "INCIDENTE DE INCOMPETENCIA EN AUTOS "NN, NN SOBRE 172 - ESTAFA"" - 17/08/2022.

ACCEDER

BENEFICIARIO DE PREMIO *(VISHING).*

HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 128829/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS "NN, (MURUA LUIS ALBERTO) SOBRE 173 INC. 15 - DEFRAUDACIÓN MEDIANTE EL USO NO AUTORIZADO DE DATOS S/ CONFLICTO DE COMPETENCIA"" - 17/08/2022.

ACCEDER

[1] Fallos vinculados con : Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires - Expte. N° INC 203098/2021-1 - "Incidente de incompetencia en autos "NN, NN sobre 173.16 - Estafa informática" - 17/08/2022.

LLAMADO TELEFÓNICO.

OFRECIMIENTO DE PRÉSTAMO SIN INTERESES *(VISHING).*

HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 127041/2022-0 - "NN, NN SOBRE 172 - ESTAFA S/ CONFLICTO DE COMPETENCIA" - 17/08/2022.

ACCEDER

INSTAGRAM.

TOKEN / HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 126409/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS N.N. SOBRE 173 INC. 16 - DEFRAUDACIÓN INFORMÁTICA S/ CONFLICTO DE COMPETENCIA" - 17/08/2022.

ACCEDER

LLAMADO TELEFÓNICO SIMULANDO SER PERSONAL BANCARIO *(VISHING).*

TOKEN / HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 75878/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS FERNÁNDEZ, CRISTIAN SOBRE 172 - ESTAFA S/ CONFLICTO DE COMPETENCIA" - 17/08/2022.

ACCEDER

LLAMADO TELEFÓNICO SIMULANDO SER PERSONAL BANCARIO. ATAQUE COMBINADO DE INGENIERÍA SOCIAL.

TOKEN / HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 26221/2022-1 - "INCIDENTE DE INCOMPETENCIA EN AUTOS "A DETERMINAR, NN SOBRE 172 - ESTAFA"" - 17/08/2022.

ACCEDER

VENTA DE BIENES.

LLAMADO TELEFÓNICO (VISHING).

TOKEN / HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 132497/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS N,N. SOBRE 173 INC. 16 - ESTAFA INFORMÁTICA S/ CONFLICTO DE COMPETENCIA" - 17/08/2022.

ACCEDER

ATAQUE COMBINADO DE INGENIERÍA SOCIAL.

BLOQUEO DE *HOMEBANKING.*

LLAMADO TELEFÓNICO SIMULANDO SER PERSONAL BANCARIO.

SMS.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 126160/2022-0 - "AGUIRRE, ROCÍO DANIELA SOBRE 173 INC. 15 - DEFRAUDACIÓN MEDIANTE EL USO DE TARJETAS DE COMPRA, CRÉDITO O DÉBITO S/ CONFLICTO DE COMPETENCIA" - 24/08/2022.

ACCEDER

MANIPULACIÓN DE CUENTA BANCARIA DE PERSONA FALLECIDA.

HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 119866/2022-0 - "ACOSTA, MIGUEL ÁNGEL Y OTROS SOBRE 173 INC. 15 - DEFRAUDACIÓN MEDIANTE EL USO DE TARJETAS DE COMPRA, CRÉDITO O DÉBITO S/ CONFLICTO DE COMPETENCIA" - 24/08/2022.

ACCEDER

REDES SOCIALES.

TARJETAS DE CRÉDITO.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 124679/2022-0 "INCIDENTE DE COMPETENCIA EN AUTOS GÓMEZ, MARCELA VIVIANA SOBRE 173 INC. 15 - DEFRAUDACIÓN MEDIANTE EL USO DE TARJETAS DE COMPRA, CRÉDITO O DÉBITO S/ CONFLICTO DE COMPETENCIA" - 07/09/2022.

ACCEDER

INSTAGRAM.

DATOS BANCARIOS.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 270428/2022-0 "INCIDENTE DE COMPETENCIA EN AUTOS MARTÍNEZ RICARDO SOBRE 172 - ESTAFA S/ CONFLICTO DE COMPETENCIA" - 07/09/2022.

ACCEDER

VENTA DE BIENES.

MARKETPLACE / FACEBOOK.

HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 247284/2021-1 - "OTROS PROCESOS INCIDENTALES EN AUTOS "DESCONOCIDO, NN SOBRE 173 15 - ESTAFA MEDIANTE EL USO DE TARJETA MAGNÉTICA O DE SUS DATOS" - 07/09/2022.

ACCEDER

GOOGLE. MENSAJES MEDIANTE *WHATSAPP* SIMULANDO SER PERSONAL BANCARIO.

TRANSFERENCIAS BANCARIAS.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 137341/2022-0 "INCIDENTE DE COMPETENCIA EN AUTOS SAAVEDRA, ANDREA DE LOS ÁNGELES SOBRE 172 - ESTAFA S/ CONFLICTO DE COMPETENCIA" - 21/09/2022.

ACCEDER

VENTA DE MONEDA EXTRANJERA.

SUPLANTACIÓN DE IDENTIDAD.

WHATSAPP / FACEBOOK.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 125313/2022-1 "INCIDENTE DE INCOMPETENCIA EN AUTOS "NN, NN SOBRE 153 1 Y 2 PÁRR. - VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD" - 28/09/2022.

ACCEDER

BENEFICIARIO DE IFE - ANSES.

WHATSAPP (VISHING).

HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 127150/2022-0 "INCIDENTE DE COMPETENCIA EN AUTOS N. N-, TEJERINA ALEJANDRO Y OTROS SOBRE 172 - ESTAFA - ART. 173 INC. 16 CP S/ CONFLICTO DE COMPETENCIA" - 12/10/2022.

ACCEDER

BENEFICIARIO DE PREMIO *(VISHING).*

TOKEN / HOMEBANKING.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 292497/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS CHÁVEZ, CRISTIAN VALENTÍN (SAMSUNG) SOBRE 173 INC. 16 - DEFRAUDACIÓN INFORMÁTICA S/ CONFLICTO DE COMPETENCIA"" - 19/10/2022.

ACCEDER

VENTA DE MONEDA EXTRANJERA.

SUPLANTACIÓN DE IDENTIDAD.

WHATSAPP.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° TSJ 299239/2022-0 - "INCIDENTE DE COMPETENCIA EN AUTOS CHACÓN, CARLOS ALBERTO SOBRE 173 INC. 16 - DEFRAUDACIÓN MEDIANTE TÉCNICA DE MANIPULACIÓN INFORMÁTICA QUE ALTERE EL NORMAL FUNC. DE UN SISTEMA INFORMÁTICO O LA TRANSMISIÓN DE DATOS S/ CONFLICTO DE COMPETENCIA"" - 26/10/2022.

ACCEDER

VENTA DE MONEDA EXTRANJERA.

SUPLANTACIÓN DE IDENTIDAD.

WHATSAPP.

ART. 172 CP.

TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES - EXPTE. N° INC 136452/2022-1 "INCIDENTE DE INCOMPETENCIA EN AUTOS "ALDERETE, MARÍA TATIANA SOBRE 172 - ESTAFA"" - 17/11/2022.

ACCEDER

JURISPRUDENCIA

ANEXO Nº 2

SENTENCIAS Y DECISIONES DE INTERÉS

En este anexo se agrupan resoluciones emanadas de órganos judiciales y administrativos que, si bien no encuadran exactamente en los ejes centrales de OCEDIC, se circunscriben a hechos cometidos en el ciberespacio que guardan un vínculo con ellos y que pueden resultar de gran utilidad para el público del Observatorio.

ARGENTINA

DERECHO AL OLVIDO.

BUSCADORES.

LIBERTAD DE EXPRESIÓN.

CORTE SUPREMA DE JUSTICIA DE LA NACIÓN - EXPTE. N° CIV 50016/2016/1/RH1 - "DENEGRI, NATALIA RUTH C/ GOOGLE INC. S/ DERECHOS PERSONALÍSIMOS: ACCIONES RELACIONADAS" - 28/06/2022[1].

La CSJN revocó sentencia que hizo lugar a demanda que había dispuesto que Google suprimiera de sus buscadores publicaciones donde la actora estaba vinculada con hechos que tuvieron lugar hace más de 20 años. Resultó decisivo en el fallo la falta de existencia de espacio suficiente para producir una lesión ilícita del derecho al honor mediante la difusión de información veraz vinculada con un asunto de interés público y referida a una persona pública que autorice una restricción al ejercicio de otro derecho fundamental como lo es la libertad de expresión.

ACCEDER

IRLANDA

RGPD[2].

DPC.

SANCIÓN ADMINISTRATIVA.

DATA PROTECTION COMMISSION (DPC) - DPC INQUIRY REFERENCE: IN-20-7-4. 02/09/2022.

La DPC de Irlanda ha impuesto una multa de 405 millones de euros a META tras una investigación sobre su gestión de los datos de menores.

Entre otras cuestiones, la decisión se basa en que Instagram habría permitido a los niños gestionar cuentas comerciales, que mostraban el número de teléfono y la dirección de correo electrónico del titular de la cuenta, exponiendo así los datos de los menores. Asimismo, se lo multa en virtud de que las cuentas de usuarios de entre 13 y 17 años estaban configuradas como "públicas" por defecto.

ACCEDER

[1] Sobre este tema, ver también :https://ocedic.com/caso-denegri-google-inc/
[2] Reglamento General de Protección de Datos (Unión Europea)

FRANCIA

RGPD.

CNIL.

SANCIÓN ADMINISTRATIVA.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)- DÉLIBÉRATION DE LA FORMATION RESTREINTE N° SAN-2022-018. 08/09/2022.

La CNIL ha impuesto una sanción administrativa de 250.000 euros al grupo de interés económico INFOGREFFE por haber infringido varias obligaciones del RGPD relativas a la conservación de datos durante un plazo proporcionado a la finalidad del tratamiento (artículo 5.1.e del RGPD) y el incumplimiento de la obligación de garantizar la seguridad de los datos personales (artículo 32 del RGPD).

ACCEDER

ARGENTINA

HABEAS DATA.

DERECHOS PERSONALÍSIMOS.

LIBERTAD DE EXPRESIÓN.

BUSCADORES.

ALGORITMOS.

CÁMARA CIVIL Y COMERCIAL FEDERAL SALA I - EXPTE. N° CCF.2091/2022/-CA1 I "S., J. M. C/ GOOGLE INC. S/ HABEAS DATA (ART. 43 C.N.) - 22/09/2022.

Se revocó resolución de primera instancia que había denegado pretensión cautelar al entender que la medida solicitada no limita el acceso a información alguna relativa al actor y por tanto no es susceptible de restringir la búsqueda, recepción y difusión de ideas a través del servicio de Internet, comprendida dentro de la garantía constitucional que ampara la libertad de expresión. El actor sustentó la procedencia de la medida precautoria en el daño que le ocasiona el hecho de que el buscador de Google sugiera -ante la introducción de su nombre- su vinculación con casos de mala praxis. En ese sentido, alegó que la relación que efectúa el algoritmo del buscador provoca una percepción distorsionada de su actividad profesional.

ACCEDER

ARGENTINA

RELACIÓN DE CONSUMO.

TRANSFERENCIAS ELECTRÓNICAS.

INVERSIÓN DE LA CARGA DE LA PRUEBA.

CÁMARA DE APELACIONES EN LO CIVIL Y COMERCIAL SALA I, ADSCRIPCIÓN N°2 DE SALTA - "L., M. E. VS. B. M. S.A. – ACCIONES DE LEY DE DEFENSA DEL CONSUMIDOR" - EXPTE. N° 688.537/19 - 10/2022.

La Sala I de la Cámara de Apelaciones en lo Civil y Comercial de Salta revocó una sentencia de primera instancia haciendo lugar a una demanda por daños y perjuicios y condenando a una entidad bancaria como consecuencia de una transferencia electrónica que nunca llegó a la cuenta bancaria de destino elegida por el actor. El fallo resaltó que el sistema de transferencias bancarias presenta peculiaridades propias y resulta innegable que el demandado, por su carácter profesional, ejerce una posición dominante respecto del cliente y, por ese motivo, se le exige un mayor compromiso en la relación de consumo. Asimismo, se puntualizó que quien se encontraba en mejores condiciones de acreditar el "circuito" del sistema de transferencia electrónica era la institución bancaria demandada y en el caso concreto, no lo hizo.

ACCEDER

FRANCIA

RGPD.

CNIL.

SANCIÓN ADMINISTRATIVA.

RECONOCIMIENTO FACIAL.

CLEARVIEW AI.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)- RESTRICTED COMMITTEE DELIBERATION NO. SAN-2022-019. 17/10/2022.

La investigación llevada a cabo por la CNIL reveló varias infracciones del RGPD, entre ellas, procesamiento ilegal de datos personales (incumplimiento del artículo 6 del RGPD) pues la recopilación y el uso de datos biométricos se llevan a cabo sin una base legal; como la falta de consideración de los derechos de las personas de manera efectiva y satisfactoria, en particular las solicitudes de acceso a sus datos (artículos 12, 15 y 17 del RGPD). Tras una notificación formal que quedó sin respuesta, la CNIL impuso una sanción de 20 millones de euros, ordenó a CLEARVIEW AI que dejara de recopilar y utilizar datos sobre personas en Francia sin una base legal y eliminar los datos ya recopilados.

ACCEDER

ARGENTINA

HABEAS DATA.

BUSCADORES.

LIBERTAD DE EXPRESIÓN.

CÁMARA NACIONAL DE APELACIONES EN LO CIVIL Y COMERCIAL FEDERAL SALA II - EXPTE. N° 7735/2016 - "MACIEL, NICOLÁS C/ GOOGLE INC. S/ HABEAS DATA (ART. 43 CN)" - 20/10/2022.

Se desestimó recurso de apelación interpuesto por parte actora contra resolución que no hizo lugar a acción de habeas data contra la empresa Google Inc. donde se solicitaba que se eliminen del motor de búsqueda de la empresa demandada noticias publicadas en medios de prensa en las que se la menciona y asocia con actividades delictivas. Los fundamentos de la decisión se centraron en la preeminencia de la libertad de expresión sobre otros derechos constitucionales.

ACCEDER

ESPAÑA

DERECHO AL HONOR.

LIBERTAD DE EXPRESIÓN: COMENTARIOS DE TERCEROS EN *FACEBOOK.*

TRIBUNAL SUPREMO. SALA CIVIL (PLENO) - STS 3970/2022. 03/11/2022.

El Tribunal Supremo considera al recurrente responsable de la ilegítima intromisión al honor, porque permitió que los comentarios publicados por los terceros en su perfil público permanecieran en él, en vez de eliminarlos, que es lo que debía haber hecho al tener un cabal y completo conocimiento de su contenido, manifiestamente atentatorio contra el honor de los recurridos, sino también un poder de control y decisión sobre su perfil que le legitimaba, igual que había hecho con otros, para borrarlos.

La responsabilidad del recurrente por no eliminarlos de su perfil público, una vez conocidos, no puede ser excusada por falta de legitimación, peligro de censura o dificultades de ponderación, puesto que existe un deber de diligencia reactiva y cuidado que le obliga, ejercitando su poder de control, a su borrado inmediato. Y si no actúa y se desentiende, incumple ese deber, convirtiéndose en responsable de los daños y perjuicios causados a título de culpa por omisión derivada de dicha falta de diligencia y cuidado.

ACCEDER

IRLANDA

RGPD.

DPC.

SANCIÓN ADMINISTRATIVA.

DATA PROTECTION COMMISSION (DPC) - DATA PROTECTION COMMISSION REFERENCE: IN-21-4-2. 25/11/2022.

La DPC de Irlanda ha impuesto una multa de 265 millones de euros a Meta Platforms Ireland Ltd. (MPIL), por la infracción de los arts. 25(1) y 25 (2) del RGPD que establecen la obligación de la protección de datos desde el diseño y por defecto.

La investigación se inicia a partir del descubrimiento de la exposición de una serie de datos personales de usuarios de Facebook.

Asimismo, de conformidad con el art. 58 (2)(d) del RGPD se ordena a MPIL que las operaciones de tratamiento de datos se ajusten a las disposiciones del Reglamento, en la forma especificada en la Decisión, dentro de los tres meses de la fecha de notificación de cualquier decisión final.

ACCEDER

ARGENTINA

HABEAS DATA.

VIOLENCIA DE GÉNERO.

LIBERTAD DE EXPRESIÓN.

BUSCADORES.

CÁMARA FEDERAL DE BAHÍA BLANCA - EXPTE. N° FBB 010089/2020/1 - "INCIDENTE N° 1 - ACTOR: B., H. A. DEMANDADO: GOOGLE ARGENTINA SRL S/ INC APELACIÓN" - 06/12/2022.

La Cámara Federal de Bahía Blanca revocó decisión de primera instancia que había resuelto hacer lugar a una medida cautelar contra Google por medio de la cual la demandada debería proceder a realizar las actividades informáticas necesarias para lograr el bloqueo provisorio de las publicaciones vinculadas a la imagen y datos personales del actor por cualquier medio digital, electrónico o gráfico; como así también la eliminación, anulación, borrado y/o desacreditación de todos los registros informáticos de imágenes, datos, comentarios, links, historiales y vínculos y la eliminación de toda frase o palabra que permita el acceso a la información en referencia a una causa penal a través de su buscador.

La resolución tuvo en cuenta que la denuncia pública de actos que podrían constituir violencia de género son de suma gravedad, por ese motivo se encuentra entre los discursos especialmente protegidos y no resultan susceptibles de restricción.

ACCEDER


LEGISLACIÓN

LEGISLACIÓN
AVANCES NORMATIVOS

En esta sección vas a encontrar un compendio de distintos tipos de normas que hayan entrado en vigencia desde junio de 2022 hasta el presente[1], así como textos complementarios, proyectos y avances en la reglamentación de temas vinculados con cibercrimen y evidencia digital, fundamentalmente con los ejes del OCEDIC, a nivel nacional (derecho argentino) e internacional. Compartimos una breve reseña y un link para acceder al material.

CIBERACOSOS A NIÑOS, NIÑAS Y ADOLESCENTES

ARGENTINA

DECRETO 407/2022. REGLAMENTACIÓN DE LA LEY N° 27.590 ("MICA ORTEGA")

Programa nacional de prevención y concientización del grooming o ciberacoso contra niñas, niños y adolescentes

14 DE JULIO 2022

ESTADO: APROBADO. REGLAMENTACIÓN

Su principal objetivo es prevenir, sensibilizar y generar conciencia en la población sobre la problemática del grooming o ciberacoso contra niñas, niños y adolescentes, a través del uso responsable de las Tecnologías de la Información y de la Comunicación (TICs), así como la capacitación de la comunidad en su conjunto.

ACCEDER

VER TAMBIÉN

ARGENTINA

PROYECTO LEY - N DE EXPEDIENTE 0051-P-2022

Imprescriptibilidad de las diferentes modalidades de abuso sexual en la infancia

21 DE JULIO 2022

ESTADO: PRESENTADO ANTE LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA

El proyecto de ley pretende lograr la imprescriptibilidad de todas las formas de violencia sexual padecida en la infancia y adolescencia y un cambio de denominación del delito. Asimismo, el 3 de agosto se anexó dentro del marco del artículo 4 el pedido de creación de una Comisión de la Verdad y reparación para los y las sobrevivientes[2].

ACCEDER

[1] Este primer número contiene excepcionalmente contenidos seleccionados en un semestre. Los próximos serán ediciones trimestrales.
[2] En similar sentido, se deja constancia de la existencia de un Proyecto de Ley anterior (Expediente: 4788-D-2020), del año 2020, que se encuentra desde entonces en "Comisiones de Cámara de Origen". CONSULTAR

CHILE

PROYECTO DE LEY. BOLETÍN N° 14.440-07

Introduce un nuevo párrafo en el Título VII del Libro II del Código Penal, relativo a la explotación sexual comercial y material “pornográfico”[3] de niños, niñas y adolescentes

21 DE NOVIEMBRE 2022

ESTADO: TRÁMITE DE FINALIZACIÓN EN CÁMARA DE ORIGEN/C. DIPUTADOS

El presente proyecto propone, entre otras cuestiones, cambiar dentro del artículo 367, la figura de la "prostitución" a la "explotación sexual" de una persona menor de dieciocho años. Define este último concepto como la utilización de una persona menor de dieciocho años para la realización de una acción sexual o de una acción de significación sexual con ella a cambio de cualquier tipo de retribución. Por otro lado, propone modificar el artículo 367 bis, eliminando la alusión al término "servicios sexuales", en razón de no ser un término descriptivamente operativo, porque puede dar a entender que la víctima es un "prestador". Luego, propone eliminar el piso de edad de catorce años para este delito y se excluye el caracter especial subsidiario en relación a los delitos de violación y estupro. Esto, además de tener sentido como declaración de principios, permite que exista un concurso ideal entre las figuras de abuso propio y esta figura de explotación sexual. Asimismo, introduce modificaciones y adecuaciones en aspectos procesales y en otros textos legales, como la ley N° 21.057, que regula las entrevistas grabadas en video y medidas de resguardo a menores de edad, víctimas de delitos sexuales.

ACCEDER

VER TAMBIÉN

REPÚBLICA DOMINICANA

PROYECTO DE LEY DE EXTINCIÓN DE DOMINIO

14 DE JULIO 2022

ESTADO: APROBADO EN SEGUNDA LECTURA POR EL SENADO

El objetivo principal es recuperar los bienes que provengan directa o indirectamente de un hecho ilícito realizado en el territorio nacional o en el extranjero. La extinción de dominio constituye una herramienta para la persecución de los activos obtenidos a través del crimen organizado, la corrupción y otras actividades criminales. El proyecto enumera, entre las causales de procedencia, los bienes respecto de los cuales procederá la acción de extinción de dominio. En este sentido, el art. 12.12 hace referencia a los bienes existentes en el territorio nacional vinculados a personas contra las cuales se ha pronunciado condena penal en el extranjero por distintos hechos, incluyendo la explotación sexual de menores, más precisamente la "pornografía infantil".

ACCEDER

[3] Se utiliza el término pornografía infantil y derivados con el uso de comillas en los casos en los que la norma o el proyecto se refiere de esta forma al material de abuso sexual infantil (MASI).

UE

PROPUESTA DE REGLAMENTO PARA PREVENIR Y COMBATIR EL ABUSO SEXUAL INFANTIL

Opinión del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos sobre la propuesta de reglamento

ADOPTADA EL 28 DE JULIO 2022

La Junta Europea de Protección de Datos (JEPD) y el Supervisor Europeo de Protección de Datos (SEPD) adoptaron un dictamen conjunto sobre la propuesta de Reglamento del 11 de Mayo de 2022 para prevenir y combatir el abuso sexual infantil (actualmente se encuentra remitido al Parlamento para su evaluación). La propuesta tiene por objeto imponer a los proveedores de servicios de alojamiento, servicios de comunicación interpersonal, tiendas de aplicaciones informáticas, servicios de acceso a Internet y otros pertinentes, obligaciones relacionadas con la detección, la notificación, la retirada y el bloqueo de material conocido y nuevo de abuso sexual infantil en línea, así como la captación de niños. Tanto el SEPD como la JEPD consideran que las restricciones a los derechos a la vida privada y a la protección de datos deben limitarse a lo estrictamente necesario y proporcionado. Si bien apoyan los objetivos y las intenciones que subyacen a la propuesta, expresan su extensa preocupación por las repercusiones de las medidas previstas en la intimidad y los datos personales. Ambos organismos aconsejan trabajar sobre la falta de detalle, claridad y precisión del texto, por ejemplo, sobre las condiciones para la emisión de una orden de detección de MASI y de la captación de menores para que la propuesta no se convierta en la base de un escaneo generalizado e indiscriminado del contenido de prácticamente todos los tipos de comunicaciones electrónicas.

ACCEDER - MÁS INFO - VER REGLAMENTO[4]

VIOLENCIA DIGITAL

ARGENTINA

PROYECTO LEY OLIMPIA - EXPEDIENTE: 2756-D-2022

Propone una modificación a la ley de Violencia de Género (26.485) para incorporar a la Violencia Digital como una modalidad de Violencia de Género

3 DE JUNIO 2022
ESTADO: EN COMISIONES DE CÁMARA DE ORIGEN (CÁMARA DE DIPUTADOS DE LA NACIÓN)

El proyecto define el concepto de “violencia digital o en línea” como aquella que se ejerce mediante el uso de las tecnologías de la información y la comunicación (TIC), y que implique la obtención, reproducción y difusión por cualquier medio de datos personales, material digital real o simulado, íntimo o de desnudez de las mujeres, sin su consentimiento, discursos de odio de género, patrones estereotipados sexistas, o que impliquen situaciones de acoso, amenaza, extorsión o control virtual, o acciones que atenten contra la integridad sexual o identidad digital de las mujeres a través de las TIC, así como cualquier otra que pueda surgir a futuro ejercida por este medio, que afecte los derechos protegidos que se indican en el texto[5].

ACCEDER

[4] Avances al cierre de esta edición: VER
[5] Sobre esta temática existen propuestas alternativas elaboradas con anterioridad al lapso tomado como parámetro para la selección de contenidos de esta publicación, pero que no han prosperado hasta el momento de finalizar la edición de la misma.

ARGENTINA

PROYECTO LEY BELÉN - EXPEDIENTE: 2757-D-2022

Propone un cambio en el Código Penal para sancionar y hacer punible la difusión como asimismo la obtención de material íntimo sin consentimiento

3 DE JUNIO 2022

ESTADO: EN COMISIONES DE CÁMARA DE ORIGEN (CÁMARA DE DIPUTADOS DE LA NACIÓN)

El texto tiene como objetivo castigar la obtención, extorsión y difusión no consentida de material íntimo y/o de desnudez, y/o de material que retrata violencia sexual y/o de "porn deep fake". Todas estas prácticas dañosas constituyen distintas formas de violencia de género digital.

ACCEDER

ARGENTINA

PROVINCIA DE BUENOS AIRES - PROYECTO DE LEY : E 150 2021-2022

Impulsa la regulación como contravención de la difusión no consentida de imágenes de carácter íntimo, el hostigamiento digital y la suplantación de identidad

28 DE JULIO 2022

ESTADO: EN ESTUDIO EN LA COMISIÓN DE LEGISLACIÓN GENERAL

Propone incorporar al Decreto Ley 8.031/73 (Código de Faltas de la Provincia de Buenos Aires) un capítulo destinado a sancionar las faltas cometidas por medios digitales con la finalidad de salvaguardar el derecho a la preservación de la intimidad, la imagen, la identidad digital, entre otros, introduciendo como contravenciones ciertas conductas para que, en el ámbito de la Provincia de Buenos Aires, puedan ser sancionadas, siempre y cuando ellas no se encuentren tipificadas como delitos de índole penal. Una de las conductas que se pretende penar es la publicación, difusión, distribución, cesión o puesta al alcance de un tercero, de imágenes, audios, textos, correos electrónicos, cuyo contenido resulte de carácter íntimo sin el consentimiento de la persona afectada. Otras conductas disvaliosas a las que se les impone un reproche punitivo contravencional son el hostigamiento y el acoso digital o ciberacoso. La tercera conducta es la apropiación, suplantación de la identidad de una persona humana o jurídica, el uso de su imagen, como así también la creación de una identidad digital “falsa”.

ACCEDER

ARGENTINA

CORRIENTES - LEY Nº 6610

Protocolo de actuación policial en materia de violencia de género

30 DE AGOSTO 2022

ESTADO: PUBLICADA EN BOLETÍN OFICIAL N° 28598

Incorpora el artículo 10 bis al Anexo I de la Ley Provincial N° 6268. En los procedimientos judiciales con temáticas que abordan violencia de género, tanto en materia penal como en lo vinculado con las normas del derecho de familia, las denuncias penales por violencias de género podrán ser realizadas mediante el sistema de "denuncia on line" del Ministerio Público de la Provincia de Corrientes.

ACCEDER

INTERNACIONAL

ESPAÑA

DISPOSICIÓN 14.630. LEY ORGÁNICA 10/2022, DE 6 DE SEPTIEMBRE, DE GARANTÍA INTEGRAL DE LA LIBERTAD SEXUAL

"Solo sí es sí"[6]

7 DE SEPTIEMBRE 2022

ESTADO: PUBLICADO EN BOE, NÚM. 215. ENTRADA EN VIGOR EL 7 DE OCTUBRE 2022

La presente ley pretende dar respuesta especialmente a las violencias sexuales cometidas en el ámbito digital, lo que comprende la difusión de actos de violencia sexual, la pornografía no consentida y la infantil en todo caso, así como la extorsión sexual a través de medios tecnológicos. De esta forma, el Código Penal Español sanciona abrir perfiles falsos en redes sociales o páginas de contacto que generen acoso o humillación a la víctima.

ACCEDER

JAPÓN

PROYECTO DE LEY NO. 208 DE MODIFICACIÓN PARCIAL DEL CÓDIGO PENAL

Cámara de Consejeros Nº 28 - Cámara legislativa superior de Japón

13 DE JUNIO 2022

APROBADO POR EL PARLAMENTO. ENTRADA EN VIGOR EL 7 DE JULIO DE 2022[7]

La cámara ha actualizado su código penal en medio de la creciente preocupación pública por el ciberacoso. La norma pretende mitigar los insultos en línea, disuadir campañas de odio y proteger a las personas de ser denigradas públicamente en plataformas digitales. Antes de la enmienda, la ley japonesa permitía 30 días de prisión por insultos, o multas de hasta 10.000 yenes (75 dólares). Ahora la ley permite hasta un año de prisión e impone un límite máximo de 300.000 yenes (2.200 dólares) en las multas. Un requisito fundamental para que la misma se apruebe, fue la adición de una disposición que ordenaba reexaminar la ley tres años después de su entrada en vigor para calibrar su impacto en la libertad de expresión.

ACCEDER

6 Ver también ensayo vinculado en este número: *"Ley integral de libertad sexual, modificación del artículo 178 del Código Penal Español, frente al llamado Yes Model, la Sexual Offences Act 2003 y el Convenio de Estambul. Breves críticas y consideraciones".*

7 Fuente: ACCEDER

INTELIGENCIA ARTIFICIAL Y HERRAMIENTAS DISRUPTIVAS DE INVESTIGACIÓN EN EL DERECHO PENAL Y PROCESAL PENAL

ARGENTINA

MENDOZA - EXPEDIENTE Nº 76092

Proyecto de modificación del Código Procesal Penal de la Provincia

2 AGOSTO 2022[8]
ESTADO: APROBADO POR LA CÁMARA DE SENADORES

El Senado aprobó el proyecto que tiene por finalidad modificar el Código Procesal Penal de la provincia incorporando normativa sobre evidencia digital y técnicas modernas de investigación en la legislación local.
La iniciativa plantea, además, la necesaria adecuación de la legislación al Convenio de Budapest de 2001 sobre ciberdelincuencia. De esta manera, se incorporará a la Ley 6730 –Código Procesal Penal- los artículos 29 bis, 216 bis, 220 bis, 220 ter, 220 quater, 224 bis y 224 ter. Uno de los puntos clave que plantea es el de agregar la figura del agente encubierto Informático. Para ello el Fiscal podrá requerir ante el Juez de Garantías la actuación de dicho agente. La autorización de este medio de investigación excepcional, se emitirá -por decreto fundado-, en el marco de la investigación de un delito.

ACCEDER

ARGENTINA

MINISTERIO DE SEGURIDAD DE LA NACIÓN - RESOLUCIÓN 720/2022

Deroga la Resolución Ministerial Nro. 144 del 31 de mayo de 2020 y sus complementarias (Prevención del delito a través de fuentes abiertas)

27 DE OCTUBRE 2022
ESTADO: VIGENTE. PUBLICADA EN EL BOLETÍN OFICIAL EL 31 DE OCTUBRE 2022

La Resolución Nro. 144 tenía como objeto regular la prevención del delito a través de fuentes digitales abiertas. La misma fue dictada durante el período en que la pandemia obligó al Estado Nacional a restringir parcialmente la movilidad. Su finalidad inicial era “la prevención policial del delito en el espacio cibernético cuyo acaecimiento sea previsible en función de la pandemia” y, por ello, la vigencia del documento se encontraba sujeta a la duración de la emergencia sanitaria. La necesidad actual de realizar tareas investigativas en medios digitales únicamente puede ser viable a través del requerimiento de la autoridad judicial competente. De esta forma, al dejar atrás dicha situación de excepcionalidad, fue incrementando exponencialmente la tensión existente entre las tareas de prevención en el medio descripto y la protección de los datos personales regulada por la Ley Nº 25.326. En este sentido, el hecho de que los datos personales objeto del protocolo en análisis se encuentren en una fuente digital abierta, no implica que quien trate esos datos no deba cumplir con los principios de calidad del dato, de información, de seguridad y de confidencialidad establecidos en la Ley mencionada ut-supra.

ACCEDER

8 VER TAMBIÉN

ARGENTINA

CORRIENTES - LEY 6518

Comienza a regir en toda la Provincia el nuevo Código Procesal Penal

8 DE NOVIEMBRE 2022
ESTADO: VIGENTE

La sanción del nuevo código fue en el año 2019. Para su implementación se adoptó la modalidad escalonada, según lo normado por el artículo 482. De esta forma, se reemplaza de modo definitivo a la Ley N° 2945 que data de 1971, y se fue implementando progresivamente en toda la provincia. Con la entrada en vigencia de la nueva norma en la Capital, toda la provincia habrá pasado del viejo sistema mixto al acusatorio adversarial.

ACCEDER

ARGENTINA

PROVINCIA DE BUENOS AIRES - PROYECTO DE LEY : E-447/22-23

Impulsa la necesidad de un abordaje multidisciplinario del delito informático

INGRESO A MESA DE ENTRADAS LEGISLATIVA EL 29 DE NOVIEMBRE 2022.
ESTADO: PRESENTADO EN CÁMARA DE SENADORES DE LA PROVINCIA DE BS. AS.

Propicia la creación de una “Comisión Bicameral para el Estudio de Propuestas Legislativas vinculadas a la Prevención, Capacitación, Investigación y Persecución Penal de Delitos concretados por medio de las Tecnologías de la Información y Comunicación (TIC’s) en el ciberespacio.
La Comisión tendrá la finalidad de armonizar la legislación procesal penal vigente, introducir nuevos medios de prueba y fomentar iniciativas necesarias que tengan como eje de trabajo los principios rectores y objetivos definidos en la Convención de Budapest. A tal fin se impulsa convocar a una mesa de trabajo multidisciplinaria. Asimismo, se hace hincapié en la prevención de estos delitos, en la capacitación de la sociedad civil y los agentes del estado, para un uso responsable de Internet y generación de recurso humano especializado en investigación.

ACCEDER

ARGENTINA

RÍO NEGRO - MINISTERIO PÚBLICO FISCAL. RESOLUCIÓN Nº 295/22/PG

Aprueba protocolo de resguardo remoto de evidencia digital

30 DE NOVIEMBRE 2022
ESTADO: VIGENTE

El denominado "Protocolo de Resguardo Remoto de la Evidencia Digital" tiene como objetivo establecer las pautas y los procedimientos que deben seguir los cuerpos técnicos forenses al momento de realizar el resguardo de evidencia digital de manera remota, sea que estén almacenados en la memoria de dispositivos (celulares, tablets, etc.) o en la "nube" (base de datos de sitios web). De esta forma se accede, descarga, resguarda y preserva de forma ágil y confiable la evidencia digital de interés para una investigación penal, sin tener la necesidad de contar físicamente con el dispositivo que contiene la información o las credenciales de acceso al lugar donde está almacenada la misma (credenciales de acceso a la "nube"). El procedimiento es sencillo y asegura la inalterabilidad de la información, por lo que puede ser incorporada a los legajos y a los juicios penales como evidencias válidas[9].

ACCEDER

INTERNACIONAL

VENEZUELA

RESOLUCIÓN CONJUNTA N-109 DE PUNTOS DE CONTROL

Evidencia digital para la transparencia de actuaciones policiales y militares

7 DE SEPTIEMBRE 2022

ESTADO: EN VIGENCIA A PARTIR DEL 8 DE SEPTIEMBRE LUEGO DE SU PUBLICACIÓN EN LA GACETA OFICIAL N°42.458 DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

El Ministerio del Poder Popular para la Defensa y el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz en compañía del Fiscal General de la Nación, emitieron una resolución conjunta que confirma el derecho de las personas a grabar los procedimientos de seguridad pública conducidos por funcionarios de organismos policiales o militares. Especifica también que las personas no tienen que entregar sus teléfonos móviles, otros grabadores o grabaciones antes, durante o después de los procedimientos. Asimismo, la resolución establece obligaciones de registro de actuaciones por parte de las autoridades. Aunque la legislación vigente (incluyendo disposiciones constitucionales) ya consideraba este derecho ciudadano, el texto pretende aclarar frente a confusiones y abusos de algunos agentes. Los registros audiovisuales obtenidos podrán ser presentados como evidencia (digital) de las condiciones e incidencias de los procedimientos.

ACCEDER - VER TAMBIÉN

9 VER

ATAQUES INFORMÁTICOS Y FRAUDE[10]

ARGENTINA

CONGRESO DE LA NACIÓN - PROYECTO DE LEY: EXPEDIENTE S-1423/2022

Acciones necesarias para la incorporación de medidas de verificación con el fin de prevenir la modalidad "SIM Swapping"

21 DE JUNIO DE 2022

ESTADO: EN COMISIONES DE LA CÁMARA DE ORIGEN

Proyecto de resolución, presentado ante la Cámara de Senadores, en el cual se solicita al Presidente del ENACOM, la implementación de medidas de verificación por parte de las empresas de telefonía móvil a los usuarios que adquieran tarjetas SIM de celulares, ante el crecimiento de casos de este tipo de fraude.

ACCEDER

ARGENTINA

CONGRESO DE LA NACIÓN - PROYECTO DE LEY: EXPEDIENTE S-221/2021

Tarjetas de crédito - Sustituye el Art. 51 de la Ley 25.065. Ref. s. 2079/19

1 DE JULIO 2022

ESTADO: EN COMISIONES DE LA CÁMARA REVISORA

Aprobado de forma unánime por la Cámara de Senadores, el proyecto (de 2021) tiene como objetivo garantizar a los usuarios de tarjetas de crédito una línea telefónica de atención permanente durante las 24 horas del día a través de una persona humana y así modificar el actual sistema de recepción de denuncias telefónicas por sustracción y pérdida de tarjetas de crédito. Asimismo, establece que el sistema deberá permitir receptar la denuncia o urgencia, mediante la mención del DNI junto con otros datos que permitan la validación de la identidad del denunciante como legítimo usuario, no pudiéndose exigir el número de la tarjeta objeto de la denuncia. Además, prevé que la atención telefónica se efectúe en un tiempo razonable.

ACCEDER

[10] Se incluye en este eje normativa vinculada con entidades bancarias y financieras a raíz del vínculo y tensiones que generan con los usuarios los ataques informáticos que involucran a las mismas.

ARGENTINA

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA - COMUNICACIÓN “A” 7593

Normas sobre “Protección de los usuarios de servicios financieros” y “Proveedores de servicios de pago”. Adecuaciones

1 DE SEPTIEMBRE 2022

SE ESTABLECE QUE LOS PUNTOS 1 Y 3 DE LA COMUNICACIÓN ENTRARÁN EN VIGOR A LOS 180 DÍAS CORRIDOS CONTADOS DESDE LA DIFUSIÓN DE LA MISMA

Por comunicación del BCRA, se incorpora a las llamadas FINTECH y las EMPRESAS QUE PRESTAN SERVICIOS DE PAGO (PSP) a las normas de protección de los usuarios de servicios financieros y quedarán equiparadas a las entidades bancarias y financieras en lo que respecta a las obligaciones que deben mantener frente a sus usuarios. Con esta comunicación, los proveedores deberán observar las normas para proteger a los usuarios del accionar de las entidades, prevenir errores o incumplimientos y promover mejores prácticas. Asimismo, encontramos que la comunicación se alinea con la Ley de Protección de Datos Personales y a los estándares internacionales de más alta jerarquía tales como los establecidos en el convenio 108 del Consejo de Europa y el RGPD. Las obligadas entre otras deberán:

I- Otorgar al usuario los medios técnicos necesarios para que, antes de la contratación, pueda detectar y subsanar eventuales errores u omisiones en la carga de los datos;

II- Proporcionarle al usuario un mecanismo de confirmación expresa de la decisión de efectuar la contratación, de forma tal que su silencio no sea considerado como consentimiento;

III- Asegurar que los términos de la contratación puedan ser leídos, descargados y guardados por el usuario de manera inalterable.

ACCEDER

ARGENTINA

PROVINCIA DE NEUQUÉN - LEY N° 3318

Tarjetas de crédito y débito - Prevención de robo de datos

3 DE ENERO 2022

ESTADO: PROMULGADA EN CUANTO A SU IMPLEMENTACIÓN, EL 1 DE SEPTIEMBRE DE 2022 SE CUMPLIÓ EL PLAZO LÍMITE PARA QUE LOS COMERCIANTES ESTÉN ALINEADOS CON LA NORMATIVA

Se prohíbe a los comerciantes que ofrecen la metodología de cobrar con el sistema de tarjetas de crédito y débito, que éstos manipulen las mismas. De esta forma, únicamente podrán solicitar a los titulares que les sean exhibidas, a fin de que puedan corroborar los datos y la firma. El objetivo es evitar posibles estafas. El incumplimiento de esta ley es motivo de sanción prevista en la ley nacional Nº 24.240 de Defensa del Consumidor.

ACCEDER

CHILE

LEY 21.459

Establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest

20 DE JUNIO 2022

ESTADO: PUBLICADA EN EL DIARIO OFICIAL DE LA REPÚBLICA DE CHILE

La ley tipifica como delitos informáticos las siguientes conductas: ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos, falsificación informática, receptación de datos informáticos, fraude informático y el abuso de dispositivos, para los cuales se contemplan penas, así como aplicación de multas. En este mismo sentido, se incorporan circunstancias modificatorias de responsabilidad penal, como el atenuante ante la cooperación eficaz, y para los supuestos donde existan agravantes, el hecho de cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función, o de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores. Por otro lado, se hacen adecuaciones de los mecanismos procesales en cuestiones de técnicas de investigación de aquellas reguladas en los artículos 222 a 226 del Código Procesal Penal, cumpliendo los requisitos previstos en la ley, y se hace referencia expresa al comiso y evidencia digital.

ACCEDER

FRANCIA

PROYECTO DE LEY DE ORIENTACIÓN Y PROGRAMACIÓN DEL MINISTERIO DEL INTERIOR

(Projet de Loi d'Orientation et de Programmation du Ministère de l'Intérieur - LOPMI)

PRESENTADO EL 7 DE SEPTIEMBRE 2022

ESTADO: ADOPCIÓN EN CURSO A LA FECHA DE CIERRE DE ESTA EDICIÓN[11]

Proyecto que ha pasado por una serie de modificaciones desde su presentación y contiene disposiciones de distinta naturaleza. En lo que respecta a la modernización de los medios de lucha contra el cibercrimen y a la "revolución digital" del ministerio, la norma prevé reformas a varios de sus códigos; en materia de criptoactivos vinculados con actividades ilícitas; en inversión destinada a ciberseguridad; en la aplicación de técnicas especiales de investigación; en mecanismos de asistencia a víctimas y denuncias online; entre otras. Cabe destacar que, en casos de ataques informáticos tales como ransomware, se atribuye la posibilidad a la víctima (en principio personas jurídicas y físicas en el marco de su actividad profesional) de obtener una indemnización por parte de su prestador de seguro condicionando la misma a la realización de la denuncia en un corto plazo. Uno de los objetivos es que las autoridades competentes dispongan de la información necesaria para perseguir a los autores de estos hechos.

TIMELINE - MÁS INFO

[11] Última versión aprobada el 7/12 por la Asamblea Nacional (consensuada en comisión mixta paritaria el 1/12). Aprobada por senadores en sesión pública el 14/12.

CHILE

LEY FINTECH. BOLETÍN N°14.570-05

Ley que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros

12 DE OCTUBRE 2022

ESTADO: APROBADO POR EL CONGRESO NACIONAL. PENDIENTE DE FIRMA DEL PODER EJECUTIVO Y DE SU PUBLICACIÓN EN EL DIARIO OFICIAL

Esta ley tiene por objeto establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos que realicen los proveedores regidos por ella. Su artículo noveno enumera las conductas que son consideradas infracciones gravísimas a las obligaciones legales en materia de protección de datos personales, tales como: efectuar tratamiento de datos personales en forma fraudulenta; destinar maliciosamente los datos personales a una finalidad distinta de la consentida; comunicar o ceder, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos; vulnerar el deber de secreto o confidencialidad sobre los datos personales sensibles; incumplir las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales, entre otras.

ACCEDER

UE

CYBERCRIME CONVENTION COMMITTEE (T-CY). NOTA ORIENTATIVA Nº 12

Aspectos del ransomware cubiertos por el Convenio de Budapest

30 DE NOVIEMBRE 2022

ESTADO: PUBLICADA

El Comité del Convenio sobre la Ciberdelincuencia (T-CY), publica notas de orientación destinadas a facilitar la aplicación efectiva del Convenio sobre la Ciberdelincuencia, a la luz de los avances jurídicos, políticos y tecnológicos. La presente nota pretende contribuir a la interpretación de dicho instrumento así como del segundo protocolo adicional frente a casos de ransomware.

ACCEDER

UE

ADHESIÓN AL CONVENIO DE BUDAPEST

NIGERIA

6 DE JULIO 2022

ESTADO: ENTRADA EN VIGENCIA A PARTIR DEL 1 DE NOVIEMBRE DE 2022

BRASIL

30 DE NOVIEMBRE 2022

ESTADO: ENTRADA EN VIGENCIA A PARTIR DEL 1 DE MARZO 2023

Durante el plazo establecido para seleccionar material para esta publicación, Nigeria y Brasil depositaron los instrumentos de adhesión al Convenio sobre Ciberdelincuencia del Consejo de Europa. Dicho texto permite, entre otros beneficios, armonizar la legislación, mejorar la cooperación internacional, proporcionar una plataforma común y herramientas de derecho procesal para investigaciones eficientes de cibercrimen, así como la preservación y la transferencia de evidencia digital según corresponda en relación a cualquier delito. Con la adhesión de ambos países, ya son 68 los Estados que pueden cooperar entre sí en el marco de este Convenio.

NIGERIA: **ACCEDER**

BRASIL: **ACCEDER - VER TAMBIÉN**

LEGISLACIÓN - ANEXO NORMATIVA DE INTERÉS

El siguiente anexo nos permite compilar avances vinculados con temáticas que se entrelazan con los ejes de OCEDIC, a pesar de no ser su objeto de estudio principal, pudiendo ser de utilidad para los lectores de LawCedic. Protección de datos personales, ciberseguridad, criptoactivos, IoT, IA aplicada en otros fueros, forman parte del material seleccionado por el equipo.

PROTECCIÓN DE DATOS PERSONALES

ARGENTINA

AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (AAIP)
PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES

Hacia la actualización normativa de la Ley 25.326

4 DE NOVIEMBRE 2022

ESTADO: PRESENTADO ANTE EL HONORABLE CONGRESO DE LA NACIÓN

Nos encontramos con un proyecto que encuentra asiento no solo en el Reglamento Europeo sobre Protección de Datos Personales (RGPD), sino que la AAIP tomó también como aporte conceptual a los más recientes estándares, recomendaciones y lecciones aprendidas en nuestra región y en el mundo durante los últimos años. Entre ellos, el Convenio 108 y su versión modernizada; las Recomendaciones de Ética de Inteligencia Artificial de la UNESCO; los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" de la Red Iberoamericana de Protección de Datos (RIPD); las legislaciones de Brasil y Ecuador; los proyectos de ley de Chile, Paraguay y Costa Rica.

ACCEDER

PROPUESTA DE ANTEPROYECTO

ARGENTINA

LEY 27.699 - DECRETO 792/2022 APROBACIÓN PROTOCOLO

Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

30 DE NOVIEMBRE 2022
ESTADO: PROMULGADA

Se formaliza legislativamente la adhesión del país al protocolo que actualizó el Convenio 108 del Consejo de Europa sobre la protección de datos de carácter personal, conocido como Convenio 108+. Constituye un avance significativo en el reconocimiento y protección de los datos personales y la autodeterminación informativa como elementos esenciales en la política de estado del país. Su objetivo es reforzar la seguridad jurídica de los ciudadanos dentro de un ecosistema socioeconómico sostenible, en el que los datos son un activo de interés público, y, por lo tanto, revisten de un valor calificado. Contempla el tratamiento de datos que supere la jurisdicción territorial y mecanismos de transferencia necesarios (extraterritorialidad).

Citamos[1] algunos lineamientos destacados:

• Se incluye un canal de comunicación para incidentes de seguridad;

• Se establecen nuevas definiciones tales como: fichero automático, tratamiento automatizado y autoridad controladora del fichero;

• Se amplía la definición de datos personales sensibles, incluyendo datos genéticos, biométricos, afiliación sindical y origen étnico;

• Se reconocen nuevos derechos para los titulares de los datos, como ser el derecho a disponer de un recurso si no se ha atendido a una petición de confirmación, comunicación, ratificación o borrado del fichero automatizado de datos de carácter personal;

• Se incluye la prohibición de tratar automáticamente datos relativos a condenas penales, origen racial, opiniones políticas, convicciones religiosas, datos relacionados con la salud y con la vida sexual;

• Se actualiza el régimen de transferencia internacional de datos, prohibiendo que un Estado parte niegue la transmisión de datos personales fuera de sus fronteras cuando el país receptor proteja los datos de manera similar al país de origen;

• Se incorporan requisitos más estrictos respecto a los principios generales sobre el tratamiento de datos, como lo es el principio de minimización de datos.

El Convenio 108+, a partir de la entrada en vigencia de la ley 27.699, integrará el derecho positivo argentino.

ACCEDER

[1] FUENTE

ARGENTINA

AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (AAIP) - RESOLUCIÓN N° 240/2022

Régimen sancionatorio en materia de datos personales

5 DE DICIEMBRE 2022

ESTADO: PUBLICADA EN EL BOLETÍN OFICIAL

La AAIP fue creada como ente autárquico con autonomía funcional en el ámbito de Jefatura de Gabinete de Ministros, con el objeto de velar por el cumplimiento de los principios y procedimientos establecidos en la Ley N° 27.275, para garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover medidas de transparencia activa y actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326. Mediante la Resolución, se derogan las Disposiciones 9 y 13 del año 2015 dictadas por la Dirección Nacional de Protección de Datos Personales, las cuales contenían el régimen sancionatorio vigente hasta la fecha. De esta forma, se actualiza el régimen por infracciones cometidas a la Ley Nacional de Protección de Datos Personales y a la Ley 26.951, mediante la cual se creó el Registro Nacional “NO LLAME”.

ACCEDER

INTERNACIONAL

ESTADOS UNIDOS

TRANSFERENCIA DE DATOS CON LA UNIÓN EUROPEA (UE)

"Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities”

7 DE OCTUBRE 2022

ESTADO: PUBLICACIÓN DE LA ORDEN EJECUTIVA EN EEUU.
POR SU PARTE EL 13 DE DICIEMBRE DE 2022, LA COMISIÓN EUROPEA COMENZÓ EL PROCESO PARA ADOPTAR LA DECISIÓN DE ADECUACIÓN PARA EL MARCO DE PRIVACIDAD DE DATOS UE-EE.UU.
EL PROYECTO DE DECISIÓN DE ADECUACIÓN SE TRANSMITIÓ AL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (CEPD) PARA QUE EMITIERA SU DICTAMEN.

Con la reciente publicación de la orden ejecutiva de la Casa Blanca, comenzará a implementarse el esperado marco de privacidad de datos entre la UE y los Estados Unidos (EE.UU.), lo cual despeja el camino tanto para los negocios como para la diplomacia transatlántica.

La orden ejecutiva exige a las autoridades de inteligencia de EE.UU. que limiten las actividades de inteligencia de señales de EE.UU. a lo que sea necesario y proporcionado. Se trata de una respuesta directa a la primera de las dos pruebas de adecuación que el TJUE consideró que el Escudo de la privacidad no superaba. De esta manera, la orden ejecutiva delimita doce "objetivos legítimos", como "la protección contra las amenazas al personal de Estados Unidos o de sus aliados", con los que deben alinearse las actividades de inteligencia de señales, y "cuatro objetivos prohibidos", como "suprimir o dificultar la crítica, la disidencia o la libre expresión de ideas u opiniones políticas".

ACCEDER

VER TAMBIÉN

BUSCADORES Y OTRAS PLATAFORMAS DIGITALES

FRANCIA

LEY N° 2022-1159

Disposiciones de adaptación al derecho de la Unión Europea en materia de prevención de la difusión de contenidos terroristas en línea (LOI no 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne)

16 DE AGOSTO DE 2022

ESTADO: PROMULGADA. PUBLICADA EN BO EL 17 DE AGOSTO

La ley adapta el derecho francés al Reglamento Europeo del 29 de abril de 2021 relativo a la lucha contra la difusión de contenidos terroristas en línea (TCO), aplicable desde el 7 de junio de 2022. El texto instaura una serie de medidas con el fin de prevenir la radicalización en Europa. En este sentido, permite imponer la obligación a los prestadores de servicios de alojamiento de datos en la UE (incluyendo Facebook, Twitter, Youtube, entre otros) de retirar o bloquear dichos contenidos en una hora (desde la recepción de la orden de retirada). Establece mecanismos para ejecutar las órdenes y llevar adelante procedimientos nacionales y transfronterizos. Los mismos deben articularse con las herramientas ya existentes en el ordenamiento interno.

ACCEDER

MÁS INFORMACIÓN

REGLAMENTO

UE

LEY DE MERCADOS DIGITALES (DMA)

Sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales)

12 DE OCTUBRE DE 2022

ESTADO: CONFORME AL ARTÍCULO 54, LA PRESENTE LEY ENTRÓ EN VIGENCIA A LOS VEINTE DÍAS DE SU PUBLICACIÓN EN EL DIARIO OFICIAL DE LA UNIÓN EUROPEA

Se aplicará a partir del 2 de mayo de 2023. No obstante, el artículo 3, apartados 6 y 7, y los artículos 40, 46, 47, 48, 49 y 50 serán aplicables a partir del 1 de noviembre de 2022 y el artículo 42 y el artículo 43 serán aplicables a partir del 25 de junio de 2023. Sin embargo, si la fecha del 25 de junio de 2022 es anterior a la fecha de aplicación a que se refiere el párrafo segundo del presente artículo, la aplicación de artículo 42 y del artículo 43 se aplazará hasta la fecha de aplicación a que se refiere el párrafo segundo del presente artículo. El presente reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

La DMA conceptualiza a las grandes plataformas de internet, que ocupan una posición dominante en el mercado digital, como "guardianes de acceso", quienes se encuentran obligados, como principio general, a evitar cualquier práctica desleal en detrimento de sus competidores más pequeños. Se les prohíbe, entre otras cuestiones, tratar datos personales de sus usuarios para remitir publicidad dirigida, sin su consentimiento; privilegiar sus propios servicios o productos dentro de sus plataformas en detrimento de terceros y establecer mecanismos que obstaculicen la desinstalación de apps preinstaladas, por defecto. De esta forma, la Comisión Europea podrá aplicar multas de hasta el 10% de la facturación mundial total del sujeto obligado, que puede ascender hasta un 20%, en caso de reincidencia. Su finalidad es hacer frente a los desequilibrios económicos que generan los grandes superintermediarios del mundo digital, sus prácticas comerciales desleales y sus consecuencias negativas, como la reducida disputabilidad comercial de los mercados de plataformas. Indirectamente, la norma busca afirmar la soberanía digital de la UE[2].

ACCEDER

2 FUENTE

UE

LEY DE SERVICIOS DIGITALES (DSA)

Relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)

27 DE OCTUBRE DE 2022
ESTADO: ENTRÓ EN VIGENCIA PASADOS LOS VEINTE DÍAS DE SU PUBLICACIÓN EN EL DIARIO OFICIAL DE LA UNIÓN EUROPEA Y SERÁ APLICADA A PARTIR DEL 17 DE FEBRERO DE 2024

La DSA tiene como principal objetivo garantizar un entorno en línea seguro, predecible y digno de confianza. Respecto a las obligaciones que impone a las "Big Tech", además de actuar con la debida diligencia, la moderación de contenidos ilegales en línea, manteniendo un delicado equilibrio entre la libertad de expresión y los derechos individuales, garantizando mecanismos internos para tramitar las quejas por contenidos retirados (que acrediten transparencia y falta de arbitrariedad) y para informar a las autoridades competentes cuando exista sospecha fundada sobre la comisión de delitos o situaciones que pongan en peligro la vida de las personas. Propone soluciones concretas a temas sensibles tales como la transparencia de los algoritmos utilizados. "Se faculta a la Comisión Europea a imponer sanciones de hasta el 6% del volumen global de los negocios del sujeto obligado (o incluso la prohibición de operar en el mercado), en caso de infracciones graves reiteradas[3]" . La norma ensaya una solución para la difusión de contenido violento, de odio, discriminatorio y/o falso (desinformación) en redes sociales o vía buscadores, y persigue garantizar la cooperación de la industria con las autoridades judiciales en la prevención y sanción de acciones delictivas.

ACCEDER

CIBERSEGURIDAD

ARGENTINA

SECRETARÍA GENERAL DE LA PRESIDENCIA DE LA NACIÓN - RESOLUCIÓN 549/2022

Política de Seguridad de la Información

22 DE AGOSTO 2022
ESTADO: PUBLICADA EN B.O.

Esta resolución define las directrices orientadas a resguardar la confidencialidad, integridad y disponibilidad de la información, protección de los recursos tecnológicos y la continuidad de las operaciones de la Secretaría General de la Presidencia de la Nación, de conformidad con las leyes y normativas vigentes.

ACCEDER

TEXTO COMPLETO

[3] Nota de Fernando Tomeo para Diario La Nación: VER

ARGENTINA

MINISTERIO DE SEGURIDAD "PARA. PIENSA. CONECTATE. ARGENTINA" RESOLUCIÓN 731/2022

Campaña federal de sensibilización pública sobre ciberseguridad y prevención del ciberdelito

1 DE NOVIEMBRE 2022
ESTADO: APROBADA POR EL PODER EJECUTIVO

En el marco de las acciones de prevención del ciberdelito del Plan Federal, se establece la generación de disertaciones y de material para ser brindados a los diferentes sectores y a la comunidad con el fin de que conozcan los riesgos que acarrean las nuevas tecnologías y sepan cómo prevenir ser víctimas de los criminales. Asimismo, se fomentan iniciativas con los organismos correspondientes tendientes a la ciudadanía digital, entre otras. El MINISTERIO DE SEGURIDAD DE LA NACIÓN, llevará adelante la conducción y coordinación de esta Campaña reforzando la concientización en ciberseguridad y proporcionando estrategias para profundizar la seguridad en el uso de herramientas tecnológicas e Internet, en conjunto con las provincias, el sector privado, los sectores académicos, las ONGs y la propia ciudadanía.

ACCEDER

INTERNACIONAL

UE

COMISIÓN EUROPEA - PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A LOS REQUISITOS HORIZONTALES DE CIBERSEGURIDAD PARA LOS PRODUCTOS CON ELEMENTOS DIGITALES Y POR EL QUE SE MODIFICA EL REGLAMENTO (UE) 2019/1020.

Proyecto tendiente a reforzar requisitos básicos de seguridad con el fin de minimizar el riesgo de ataques (Cyber Resilience Act - CRA)

15 DE SEPTIEMBRE 2022
ESTADO: PENDIENTE DE REVISIÓN POR PARTE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

La propuesta de reglamento sobre los requisitos de ciberseguridad de los productos con elementos digitales (IoT), refuerza las normas para garantizar productos de hardware y software más seguros.
Se establecieron cuatro **objetivos específicos**: 1) Garantizar que los fabricantes mejoren la seguridad de los productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida; 2) Garantizar un marco coherente de ciberseguridad que facilite el cumplimiento de las normas por parte de los fabricantes de hardware y software; 3) Mejorar la transparencia de las propiedades de seguridad de los productos con elementos digitales, y 4) Permitir que las empresas y los consumidores utilicen los productos con elementos digitales de forma segura.

ACCEDER

VER TAMBIÉN

NORMA ISO 27001. VERSIÓN 2022

Requisitos de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad

25 DE OCTUBRE 2022
ESTADO: PUBLICADA

ISO/IEC 27001 es la norma internacional para la seguridad de la información por excelencia. Esta nueva versión pretende alinear aún más el Sistema de Gestión con el Anexo SL, lo que en la práctica significa un claro interés por promover la integración con otros Sistemas. Las organizaciones contarán con tres años, es decir, hasta octubre de 2025, para ajustar sus Sistemas de Gestión al nuevo estándar y certificarlo. Fundamentalmente, la nueva ISO 27001:2022 no representa mayores modificaciones de la versión anterior. En este sentido, trae pequeños cambios de redacción, un cambio de numeración en dos controles y algunas aclaraciones. El cambio más importante es el de la norma ISO27002/Anexo A. Otros de los cambios más significativos se encuentran dentro de las secciones de contexto de la organización; planificación; soporte; operación; desempeño y evaluación. Su aplicación exitosa es un aporte al conjunto de mejores prácticas para la protección de las organizaciones frente a la complejidad creciente de los escenarios de riesgos[4].

ACCEDER

UE

RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO, DE 10 DE NOVIEMBRE DE 2022, SOBRE LA PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVA A LAS MEDIDAS DESTINADAS A GARANTIZAR UN ELEVADO NIVEL COMÚN DE CIBERSEGURIDAD Y POR LA QUE SE DEROGA LA DIRECTIVA (UE) 2016/1148 - COM(2020)0823 – C9-0422/2020 – 2020/0359(COD) -

Actualización de normas de ciberseguridad en el marco de la UE

TEXTO APROBADO POR EL PARLAMENTO EL 10 DE NOVIEMBRE DE 2022. APROBACIÓN POR EL CONSEJO EL 28 DE NOVIEMBRE DE 2022

TRÁMITE FINALIZADO EL 14 DE DICIEMBRE 2022, PENDIENTE DE PUBLICACIÓN EN DIARIO OFICIAL[5] (LA DIRECTIVA NIS2 ENTRARÁ EN VIGOR 20 DÍAS DESPUÉS DE SU PUBLICACIÓN TRAS LO CUAL LOS ESTADOS MIEMBROS TENDRÁN VEINTIÚN MESES PARA SU INCORPORACIÓN EN DERECHO INTERNO)

El Parlamento y el Consejo de la Unión Europea han aprobado un paquete de normas de ciberseguridad que establece requisitos más estrictos para las empresas, las administraciones y las infraestructuras con medidas que trabajan en pro de un alto nivel común de ciberseguridad en toda la Unión. Al actualizar la directiva sobre seguridad de las redes y de la información (NIS), el Parlamento de la UE amplía el ámbito de aplicación de la propuesta de directiva NIS2, derogando la directiva del año 2016. La NIS2 introduce nuevas normas para impulsar un alto nivel común de ciberseguridad en toda la UE, tanto para las empresas como para los países. También refuerza los requisitos de ciberseguridad para las entidades medianas y grandes que operan y prestan servicios en sectores clave.

TEXTO COMPLETO

VER TAMBIÉN

4 FUENTE
5 TIMELINE

CRIPTOACTIVOS - BLOCKCHAIN

ARGENTINA

AFIP - DICTAMEN N° 2/2022

Criptomonedas. Naturaleza jurídica. Gravabilidad. Su tratamiento

16 DE JUNIO 2022
ESTADO: PUBLICADO

Dicho texto establece que: se puede caracterizar a las criptomonedas como una nueva clase de activo financiero, no tradicional y basado en la tecnología blockchain el cual versa, en definitiva, acerca de una anotación electrónica que incorpora el derecho a una cantidad de dinero determinada, que puede tipificarse como títulos valores, toda vez que participan de las características principales que poseen estos últimos, es decir, son valores incorporados a un registro de anotaciones en cuenta –la blockchain-; resultan bienes homogéneos y fungibles en los términos del artículo 232 del Código Civil y Comercial; su emisión o agrupación es efectuada en serie –conformada ésta por cada bloque que integra la cadena- y; pueden ser susceptibles de tráfico generalizado e impersonal en los mercados financieros. Las criptomonedas conforman un activo alcanzado por la ley de Impuesto sobre los Bienes Personales de conformidad con lo prescripto en el citado artículo 19, inciso j) y artículo 22 inciso h) de la ley del gravamen.

ACCEDER

ARGENTINA

JEFATURA DE GABINETE DE MINISTROS. SECRETARÍA DE INNOVACIÓN PÚBLICA - RESOLUCIÓN 17/2022

7 DE DICIEMBRE 2022
ESTADO: VIGENTE.
PUBLICADO EN EL
BOLETÍN OFICIAL

La resolución propone, en primer lugar, crear el "Comité Nacional de Blockchain" y, en segundo lugar, aprobar el "Lineamiento Nacional Sobre Blockchain", establecido en el anexo. El documento propone sentar las bases y líneas de acción para la implementación de un "Plan Nacional De Blockchain" en Argentina.

ACCEDER

VER ANEXO

INTERNACIONAL

UE

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A LOS MERCADOS DE CRIPTOACTIVOS Y POR EL QUE SE MODIFICA LA DIRECTIVA (UE) 2019/1937

Reglamento de Mercados de Criptoactivos (MiCA)

9 DE OCTUBRE 2022

ESTADO: APROBADO EN COMISIÓN EL TEXTO ACORDADO EN 1ª LECTURA DE NEGOCIACIONES INTERINSTITUCIONALES. A LA ESPERA DE LA POSICIÓN DEL PARLAMENTO EN 1ª LECTURA

El Comité de Asuntos Económicos del Parlamento Europeo aprobó la ley MiCA y el Reglamento de Transferencias de Fondos. La ley MiCA[6] , cuyo desarrollo y debate data del 2018, pretende darle un marco legal al ecosistema. El Reglamento de Transferencias de Fondos pretende que estas operaciones sean rastreadas, es decir, que quienes transfieren y reciben sean identificados. El documento basa gran parte de su atención en los exchanges de criptomonedas. Estas empresas deberán tener una licencia y estar registradas ante las autoridades europeas para poder operar en Europa. Ejes principales de esta normativa:

- Marco jurídico uniforme para los criptoactivos en la UE;
- Protección del consumidor y salvaguardias contra la manipulación del mercado y los delitos financieros;
- Los proveedores de servicios de criptoactivos (CASP) deberán revelar su consumo de energía;
- Introducirá disposiciones sobre supervisión, protección del consumidor y salvaguardias medioambientales para los criptoactivos;

Hechos clave:

- La Ley MiCA podría entrar en vigencia en el tercer trimestre del año 2024.
- Aún debe ser revisada, debatida y aprobada por autoridades europeas.

ACCEDER

VER TAMBIÉN

BRASIL

PROYECTO LEY 4401/2021 (Nº ANTERIOR: PL 2303/2015)

Lineamientos para la regulación de la prestación de servicios de activos virtuales (criptomonedas)

29 DE NOVIEMBRE 2022

ESTADO: APROBADO POR LA CÁMARA DE DIPUTADOS. EN ESPERA DE SANCIÓN

El proyecto de ley tiene como objetivo frenar los delitos de malversación y lavado de dinero relacionados con la transacción de activos virtuales. La propuesta deja en manos del Poder Ejecutivo la designación de un órgano que actuará como regulador del mercado de las criptomonedas. En el documento, se establecen reglas para el funcionamiento de los proveedores de servicios de Bitcoin y otras criptomonedas, entre ellos los exchanges. Deja puntos claros sobre cómo los terceros de confianza deben prestar los servicios de custodia. Resulta interesante, dado que obliga a los proveedores de servicios a separar sus fondos de los de sus clientes. Por otro lado, el proyecto propone incorporar en el Art. 171-A del Código Penal, la figura de “Fraude con el uso de activos virtuales, valores o activos financieros”.

ACCEDER

SITIO WEB C. DIPUTADOS BR

VER TAMBIÉN

6 FUENTE

RESPONSABILIDAD EN MATERIA DE INTELIGENCIA ARTIFICIAL

UE

RESPONSABILIDAD EN MATERIA DE INTELIGENCIA ARTIFICIAL

La Comisión Europea ha presentado dos propuestas legislativas que introducen normas de responsabilidad para la Inteligencia Artificial (“IA”)

28 DE SEPTIEMBRE 2022

ESTADO: EL PARLAMENTO EUROPEO Y EL CONSEJO DEBERÁN APROBAR LA PROPUESTA DE LA COMISIÓN

- Revisión de la Directiva 85/374/CEE del Consejo, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos (“Directiva RPD”);
- Propuesta de una Directiva específica sobre responsabilidad en materia de IA.

Con estas propuestas, la UE pretende adaptar el régimen de responsabilidad objetiva a la era digital.

ACCEDER

VER TAMBIÉN


DOCTRINA

DOCTRINA

En general, creemos que es sumamente importante para la incorporación y adaptación de una norma a un ordenamiento jurídico el análisis doctrinario que permita reflexionar y resolver cuestiones que la misma pueda plantear. Nuestra convicción se refuerza en materia de cibercrimen y evidencia digital. En consecuencia, LawCedic te propone esta sección con el fin de contribuir a la elaboración de principios, conceptos, razonamientos, debates y recomendaciones, gracias al aporte de colaboradores expertos. En cada número seleccionamos artículos, ensayos, notas de opinión, comentarios a fallos, entre otros trabajos relacionados con las temáticas que investiga el OCEDIC, de manera tal que los miembros del equipo e invitados puedan ir participando según su especialidad.

UTILIZACIÓN DEL SOFTWARE SHOTSPOTTER: LA IA PREDICTIVA NUEVAMENTE CUESTIONADA

Antonella María Bentin[1]

Si bien los modelos predictivos más básicos se fundan en datos recopilados por la propia policía, tales como delitos denunciados y delitos descubiertos por el cuerpo policial, otros programas han pasado a incorporar factores tan variables como las ubicaciones de bares nocturnos – donde se pueden producir incidentes- y potenciales rutas de escape. Hoy en día, la policía predictiva ha evolucionado para apuntar a un espectro mucho más amplio de delitos, como robos, tiroteos y violencia relacionada con pandillas mediante el análisis de vulnerabilidades geográficas: ejemplos de ellos son PredPol, Palantir, entre otros.

En medio de un debate sobre el sesgo racial en la vigilancia, los defensores de la privacidad[2] y los derechos civiles expresan que el sistema de ShotSpotter y otras tecnologías basadas en algoritmos utilizadas para establecer sentencias de prisión hasta reglas de libertad condicional, carecen de transparencia y supervisión.

[1] Staff LawCedic. Abogada. Especialista en Derecho Penal. Maestranda en Derecho Penal (Universidad de Palermo). Diplomada en Cibercrimen e Innovación digital (Universidad de Hartmann, México). Se desempeña en el Ministerio Público de la Defensa. (bentin.antonella@gmail.com).

[2] La NACDL (National Association of Criminal Defense Lawyers) elaboró un informe respecto a la temática en el cual expresan alguno de los problemas que presenta: el uso de algoritmos predictivos producía bucles de retroalimentación auto perpetuantes de predicciones de delitos, en los que los oficiales patrullaban repetidamente los vecindarios que habían sido blanco de manera desproporcionada por parte de las fuerzas del orden en el pasado y, por lo tanto, estaban sobrerrepresentados en los datos históricos de delitos utilizados para entrenar y construir algoritmos de predicción de delitos. Ver: "Garbage in, gospel out. How Data-Driven Policing Technologies Entrench Historic Racism and 'Tech-wash' Bias in the Criminal Legal System." Publicado por NACDL, septiembre 2021.

¿QUÉ ES EL SOFTWARE SHOTSPOTTER? ¿CÓMO FUNCIONA?

El sitio web[3] de ShotSpotter explica que solo el 20% de los incidentes vinculados con disparos se denuncian por la comunidad al 911. Esto crea una situación en la que los departamentos de policía tienen una gran brecha de datos que dificulta poder "servir y proteger" de manera efectiva cuando se trata de violencia armada.

En ese sentido, ShotSpotter llena el vacío con una red de sensores acústicos que pueden detectar, ubicar y alertar a la policía sobre casi todos los incidentes de disparos. El sistema está en funcionamiento en más de 120 ciudades y la policía lo utiliza para: 1) poder responder a un mayor porcentaje de incidentes de disparos; 2) mejorar los tiempos de respuesta en las escenas del crimen para ayudar mejor a las víctimas y encontrar testigos; y 3) ayudar a la policía a localizar evidencia clave para identificar y enjuiciar a los sospechosos.

Según explica su propio sitio web, ShotSpotter utiliza dos algoritmos principales en el análisis de sonidos en tiempo real: primero, un algoritmo para determinar la ubicación de "estallidos y explosiones", y segundo, un algoritmo de aprendizaje automático para filtrar sonidos que no son de disparos.

El primer algoritmo determina la ubicación de los sonidos que se escuchan en un área en función de la velocidad del sonido y los momentos en que el sonido llega a los diferentes sensores. El segundo algoritmo utilizado para clasificar los sonidos es el que tiende a generar alarma. Luego de ello, es supervisado por personal capacitado que da aviso a la policía.

CUESTIONAMIENTOS. ACCIONES LEGALES

Sin embargo, las asociaciones de derechos civiles, como la ACLU y el Centro de Justicia MacArthur presentaron varios cuestionamientos[4]:

Primero, sostienen que la tecnología se despliega abrumadoramente en comunidades de color, que ya soportan de manera desproporcionada la presencia policial. La policía sostiene que eligen los vecindarios para el despliegue en función de dónde se encuentran la mayoría de los tiroteos, sin embargo, la ACLU entiende que hay varios problemas con eso:

1. Las falsas alarmas de ShotSpotter envían a la policía en numerosas ocasiones a las comunidades sin ningún motivo y en alerta máxima, esperando enfrentar una situación potencialmente peligrosa. Dada la trágica cantidad de muertes de personas negras en manos de la policía, eso ya es un problema, ya que en algunos vecindarios lleva a los oficiales a participar de más paradas y cacheos.

2. La colocación de sensores en algunos barrios, pero no en otros, significa que la policía detectará más incidentes (reales o falsos) en los lugares donde se encuentran los sensores. Eso puede distorsionar las estadísticas de disparos y crear una justificación estadística circular para el exceso de vigilancia en las comunidades de color.

En segundo lugar, la ACLU afirma que la metodología de ShotSpotter se utiliza para proporcionar pruebas contra los acusados en casos penales, pero no es transparente y no ha sido revisada por pares ni evaluada de forma independiente.

Otro problema que se cuestiona aún más es la idoneidad de las pruebas de ShotSpotter para su uso en los tribunales: la relación aparentemente estrecha de la empresa con las fuerzas policiales. Un experto de ShotSpotter admitió en un juicio de 2016, por ejemplo, que la compañía reclasificó los sonidos de un helicóptero a un disparo a pedido de un "cliente" del departamento de policía, diciendo que tales cambios ocurren "todo el tiempo" porque "confiamos en que nuestros clientes encargados de hacer cumplir la ley son realmente sinceros y honestos con nosotros". ShotSpotter también utiliza los informes de los agentes de policía como "verdades sobre el terreno" al entrenar su algoritmo de IA para que no cometa errores. No sorprende la estrecha relación entre ShotSpotter y la policía: los departamentos de policía son los clientes de la empresa y la empresa necesita mantenerlos contentos, sostiene la ACLU.

Sin embargo, varias ciudades han dejado de usar la tecnología después de decidir que ShotSpotter genera demasiados falsos positivos reportando disparos donde no los hubo.

[3]Sitio web de ShotSpotter https://www.shotspotter.com/company/
[4]Ver informe completo en: https://www.aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system

El 21 de julio del corriente año, se ha presentado una demanda[5] contra la ciudad de Chicago. La demanda gira en torno a un tiroteo en Chicago en 2020 en el que una persona resultó muerta. La policía vinculó ese asesinato a un hombre de 65 años llamado Michael Williams utilizando dos pruebas: según los informes, la policía obtuvo un video de seguridad sin ruido del vehículo de William pasando por una intersección, y luego se vinculó un disparo supuestamente detectado por el sistema de ShotSpotter en esa zona. Williams fue arrestado en 2021 y pasó casi un año detenido antes de que un juez finalmente desestimara su caso después de que los fiscales admitieran que carecían de pruebas suficientes[6].

La demanda acusa a la policía y los fiscales, porque nunca establecieron un motivo para que Williams le disparara a la víctima, como así tampoco recuperaron un arma o evidencia física que vincule al nombrado con el asesinato. "Los oficiales acusados se involucraron en una visión de túnel para apuntar al Sr. Williams, arrestándolo por asesinato en primer grado, sin causa probable", dice la demanda. Es decir, que los oficiales tratan a cualquier persona en el área con sospecha, a pesar de saber que la gran mayoría de las alertas de ShotSpotter no arrojan evidencia de disparos[7].

Daniel Ortiz, otra persona que consta en la presentación de la demanda, fue detenido ilegalmente, cacheado, esposado, interrogado y finalmente arrestado fuera de un local comercial por oficiales luego de una alerta infundada de ShotSpotter. Pasó la noche en la cárcel antes de que se desestimaran los cargos. De hecho, no hubo ningún disparo y la policía no encontró nada que corroborara la alerta de ShotSpotter.

El Sr. Williams individualmente pide una indemnización por los daños físicos, médicos y emocionales que sufrió mientras estuvo 11 meses encarcelado por cargos falsos. El Sr. Ortiz también busca una reparación de daños y perjuicios por su parada ilegal, arresto, detención y decomiso del vehículo. La demanda está presentada de manera colectiva para cualquier residente de Chicago que haya sido detenido en base a las alertas y, entre otras cosas, busca una orden judicial que prohíba el uso de la tecnología en Chicago.

La demanda explica que la ciudad ha cubierto 12 de los 22 distritos policiales de Chicago con ShotSpotter - casi todo el lado sur y oeste-. Estos 12 distritos son exactamente los que tienen la mayor proporción de residentes negros y latinos - y la proporción más baja de residentes blancos-. El 80% de los habitantes negros de Chicago viven dentro de la zona activa de ShotSpotter, lo que es una decisión racialmente discriminatoria.

Asimismo, expresa que ShotSpotter continúa enunciando públicamente una tasa de precisión del 97%, una estadística que sería engañosa y falsa, ya que no ha habido ninguna prueba real para ver si ShotSpotter puede distinguir de manera confiable la diferencia entre el sonido de disparos y otros ruidos como petardos, ruidos de construcción, helicópteros y otros sonidos fuertes e impulsivos. Los llamados números de "precisión" de ShotSpotter simplemente asumen que sus alertas corresponden a disparos el 100% de las veces y solo marcan una alerta como un error si la policía presenta una denuncia voluntaria. Sin embargo, en Chicago, los agentes de policía no presentan una denuncia cuando buscan una alerta de ShotSpotter y no encuentran nada, que es lo que sucede más del 90 % de las veces.

Incluso, la demanda afirma que con respecto a la ubicación de los supuestos disparos, un empleado de ShotSpotter admitió que los incidentes pueden ser "significativamente mal ubicados" por distancias de 450 metros o más.

CONCLUSIÓN

Se puede concluir que, como varias tecnologías predictivas que funcionan a través de IA y se utilizan en procesos penales, esta no sería la excepción a las críticas. Diversos estudios han concluido que los sistemas predictivos -por ejemplo, para detectar zonas donde se pueden cometer delitos,- por más que se sofistiquen, no consiguen resolver un problema central: cómo tratar de no penalizar a los barrios más desfavorecidos, o lugares donde la población se encuentra compuesta mayormente por personas negras.

Si bien la intención es que ShotSpotter sea utilizada con un buen fin, también funciona como una razón para detener y cachear a las personas en las calles y tratarlas como sospechosas delictivas solo porque supuestamente ha habido un historial de alertas de ShotSpotter en el área. Y estas áreas generalmente son barrios donde la tasa de criminalidad es mayor, generándose un círculo vicioso, que se presta a arbitrariedades por parte del personal policial.

Es por ello, que se deberá seguir pensando en el uso de este tipo de tecnologías por parte de la policía, tratando de encontrar un equilibrio justo entre la persecución penal y los derechos de los ciudadanos.

---

[5] Demanda completa en https://www.macarthurjustice.org/wp-content/uploads/2022/07/Complaint-file-stamped.pdf

[6] "The State of Illinois v. Michael Williams". Case nro. 20 CR 0899601.Court Of Cook County Criminal Division - Judge Vincent Gaughan.
Para más información de interés, ver amicus presentado en la causa:
https://endpolicesurveillance.com/documents/2021-05-03-Motion-for-Leave-to-File-Brief-as-Amici-Curiae-with-Ex.-A-Amicus-Brief-attached.pdf

[7] "Demanda: la policía de Chicago usó indebidamente ShotSpotter en un caso de asesinato". Disponible en: https://noticiasporelmundo.com/ee-uu-mundo/demanda-la-policia-de-chicago-uso-indebidamente-shotspotter-en-un-caso-de-asesinato/

CIBERESTAFAS: CONFLICTOS DE COMPETENCIA EN LA CIUDAD DE BUENOS AIRES

Juan Pablo Andueza[1]

La Ciudad Autónoma de Buenos Aires tiene la particularidad de tener dos fueros penales ordinarios con distintas competencias hasta tanto se finalice el proceso de transferencia de competencias progresivo dispuesto en la ley 24.588 (conocida como Ley Cafiero), que garantizaba los intereses del Estado Nacional mientras la CABA sea la capital de la República.

Por un lado, tenemos a la Justicia Nacional en lo Criminal y Correccional y, por el otro, a la Justicia Penal, Contravencional y de Faltas de la CABA, habiéndose efectuados distintos convenios de transferencia de delitos desde el ámbito nacional al local.

Esta situación ha llevado a distintas particularidades a la hora de determinar la distribución de competencias, por lo que en este trabajo haré un breve y actualizado análisis de las atribuciones de competencia sobre los hechos subsumibles en el delito de estafa cuando es perpetrada por medios informáticos (Art. 172 del CP) y las defraudaciones previstas en el Art. 173 inc. 15 y 16 del CP en el ámbito de la Ciudad Autónoma de Buenos Aires.

Como regla general, el Tribunal Superior de Justicia (TSJ) ha determinado que en los casos en que los hechos encuadran en el delito de estafa simple debe intervenir el Fuero Nacional en lo Criminal y Correccional[2].

En relación a las defraudaciones específicas – mediante el uso de tarjetas de crédito o débito sustraídas, adulteradas o pérdidas, u obtenidas del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos (Art. 173 inc. 15) y mediante alteración o cualquier técnica de manipulación informática del normal funcionamiento de un sistema informático o de la transición de datos (Art. 173 inc. 16)[3] "ha considerado que corresponde a la Justicia de la CABA por cuanto si bien son delitos que no se encuentran incluidos en ningún de los tres convenios de traspaso de competencias penales, aquellas disposiciones que estipulan sanciones para conductas que con anterioridad a la ley 24588 no eran objeto de persecución penal son, como principio general, de competencia del Poder Judicial de la Ciudad"[4].

[1] Staff LawCedic. Abogado. Magister en Derecho Penal por la Universidad Austral. Diplomado en Cibercrimen (2021 – Univ Austral) y en Delitos del Crimen organizado (2016 – Univ. Marín). Desempeñándose como Fiscal interino en el MPF – CABA.

[2] En materia de estafas simples – Art. 172 del CP, a saber: "Incidente de competencia en autos González, Lorena Elizabeth y otros sobre 173 inc. 15 – defraudación mediante el uso de una tarjeta de compra, crédito o débito s/ conflicto de competencia", Expte. SAPPPJCyF Nro. 237832/21-0, sentencia del 23/02/2022; "Incidente de incompetencia en autos NN, NN sobre 173.16 – estafa informática", Expte. SAPPJCyF Nro. 194244/21-1, sentencia del 20/12/2021", entre otros.

[3] "NN, NN s/ 00 – presunta comisión de delito (Art. 173 inc. 16 CP) s/ conflicto de competencia I", Expte SAPPJCyF Nro. 17891/20; sentencia del 31/03/2021, entre otros.

[4] Cuestiones de Competencia – Estafas y Otras Defraudaciones (Art. 172 y 173 inc. 15 y 16 del Código Penal) – Compilado de jurisprudencia del TSJ - agosto 2021 – Pág. 6.

En este sentido, el Fiscal General de la CABA dispuso por criterio general que los Fiscales con competencia penal, contravencional y de faltas deben asumir la competencia para investigar los tipos penales previstos en los incisos 15 y 16 del Art. 173 del CP[5].

En dicha resolución, en función del principio de autonomía judicial consagrado en el Art. 129 de la Constitucional Nacional y a lo previsto en el Art. 8 de la ley 24.588 donde se prevé la transferencia de competencias de delitos de la Justicia Nacional a la Justicia de la CABA, se valoró que todo delito sancionado con posterioridad a dicha norma será de competencia de la Justicia Local, ya que no se puede transferir un delito que nunca estuvo en la esfera de la competencia de la justicia nacional.

Vale recordar que la ley 26.702 de transferencia de competencias del año 2011, estableció expresamente que se le asigna al Poder Judicial de la Ciudad Autónoma de Buenos Aires la competencia para investigar y juzgar los nuevos delitos de competencia penal ordinaria, aplicables en su ámbito territorial, que se establezcan en lo sucesivo en toda ley de la Nación, salvo que expresamente se disponga lo contrario.

Sin embargo, el Procurador General de la Nación[6] estableció un criterio general de actuación, ordenando a los Fiscales Nacionales que deberán sostener la competencia en los casos de estafas previstas en el Arts. 173 inc. 15 y 16 del CP, considerando que no se trataba de un nuevo delito, sino de distintas modalidades de defraudación, y que ambos delitos fueron incorporados al código penal con anterioridad a la sanción de la ley 26702.

Valorando para ello, que las defraudaciones se encuentran sancionadas en el código penal desde 1921, tratándose de modalidades incorporadas en el tiempo, y que la sanción de ambas figuras es anterior al establecimiento de la ley 26702, ya que el inc. 15 del Art. 173 fue incorporado al código penal en el año 2004, mientras que el inc. 16 lo fue en el año 2008. En este sentido ya se venían expidiendo en la Cámara Nacional de Casación en lo Criminal y Correccional, entendiendo que estos incisos en particular no fueron incluidos en convenios de transferencia que fueron acordados entre la Nación y la CABA con posterioridad a su creación legislativa (véase que el tercer convenio de transferencia es del año 2011 y los delitos en cuestión fueron sancionados con anterioridad)[7].

Ahora bien, esta situación particular nos lleva a que ambos poderes judiciales con competencia en el mismo ámbito territorial se consideren competentes para intervenir en las investigaciones por el mismo delito.

Debo recordar que la propia Corte Suprema de Justicia de la Nación en el fallo BAZAN estableció que el TSJ es quien dirimiría los conflictos de competencia entre la Justicia Nacional en lo Criminal y Correccional y la Justicia de la CABA, al reconocer que la CABA debe tener plena autonomía de jurisdicción, teniendo los tribunales nacionales un carácter transitorio, tesitura apoyada en los antecedentes conocidos como "CORRALES" y "NN (VTMA NISMAN)" del Máximo Tribunal del país.

En este sentido, el primer fallo trascendental del TSJ sobre conflicto de competencia por delitos ordinarios conocido como "GIORDANO" estableció que tanto los jueces locales como nacionales pueden resolver sobre la totalidad de los delitos de competencia ordinaria, en virtud de razones de mejor y más eficiente administración de justicia para evitar conflictos entre distintos juzgados con competencia penal.

Por lo tanto, si bien considero que la Justicia de la CABA es quien debe tener la competencia en estos nuevos delitos por los motivos expuestos inicialmente por el TSJ, lo cierto es que, ante la postura establecida en el fallo mencionado y, teniendo en cuenta el carácter transitorio de la Justicia Nacional, ambos fueros podrían juzgar los hechos calificados en los delitos de defraudación específica previstos en los incisos 15 y 16 del CP como el delito de estafa simple (Art. 172 del CP), debiendo intervenir el órgano jurisdiccional que previno y evitar declinaciones de competencias para evitar dilaciones en el proceso.

Considero que esta situación no puede mantenerse en el tiempo, se debe resolver, y entendiendo que la mejor manera sería desde el plano legislativo, para dar certeza a la ciudadanía, sobre todo teniendo en cuenta que nos encontramos ante delitos que están en auge, por lo que esta división de las investigaciones puede frustrar el éxito en la determinación de los responsables y evitar que se sigan cometiendo estas defraudaciones.

5 Resolución Nro. 48/21 de FG de fecha 4/06/2021.
6 Resolución PGN 38/22 de fecha 6/06/2022.
7 Fallo Reg. 295/22 de la Cámara Nacional de Casación en lo Criminal y Correccional – sala 2. 23/03/2022.

BIBLIOGRAFÍA

• Resolución Nro. 48 de Fiscal General – MPFCABA de 4/6/2021.

• Resolución PGN 38/22 del Procurador General de la Nación de 6/6/2022.

• Dictamen de Fiscal General Adjunta – MPF CABA en Expediente No 172811/2021-0 "INCIDENTE DE COMPETENCIA EN AUTOS BENITEZ, VICTORIA ALEJANDRA SOBRE 172 - ESTAFA - ART. 173 INC. 16 CP. s/ CONFLICTO DE COMPETENCIA" de fecha 23/08/2021.

• Fallo TSJ "BENITEZ, VICTORIA" - Expte. n° TSJ 172811/2021- 0 "INCIDENTE DE COMPETENCIA EN AUTOS BENITEZ, VICTORIA ALEJANDRA SOBRE 172 - ESTAFA - ART. 173 INC. 1 CP. s/ CONFLICTO DE COMPETENCIA" de fecha 13/10/2021.

• Fallo TSJ "GIORDANO" – TSJ - Expte. no 16368/19 "Incidente de competencia en autos Giordano, Hugo Orlando y otros s/ infr. art. 89, CP, lesiones leves s/ conflicto de competencia I" – 26/10/2019.

• Fallo TSJ "BAZAN" – TSJ - Expte. nº 16327/19 "Bazán, Fernando s/ amenazas s/ conflicto de competencia I" – 11/03/2020.

• Fallo CSJN "BAZAN" – CSJN - TSJ - Expte. nº 16327/19 "Bazán, Fernando s/ amenazas s/ conflicto de competencia I" – 4/04/2019.

• Fallo CSJN "CORRALES" Competencia CCC 76l4/20l5/CNC1-Cal Corrales, Guillermo Gustavo y otro si hábeas corpus" de 9/12/2015.

• Fallo CSJN "NN – vtma Nisman" eee 3559/20l5/l6/5/l/RH8 N.N. Y otros s/ averiguación de delito - Damnificado: Nisman, Alberto y otros" de 20/09/2016.

• Fallo CNCCyC R eg. 295/22 - sala 2. 23/03/2022 s/ cuestión de competencia.

• Cuestiones de Competencia – Estafas y Otras Defraudaciones (Art. 172 y 173 inc. 15 y 16 del Código Penal) – Compilado de jurisprudencia del TSJ - Agosto 2022
https://www.tsjbaires.gov.ar/images/stories/librosdigitales/cc_estafas_otras_defraudaciones.pdf

LEY INTEGRAL DE LIBERTAD SEXUAL, MODIFICACIÓN DEL ARTÍCULO 178 DEL CÓDIGO PENAL ESPAÑOL, FRENTE AL LLAMADO *YES MODEL*, LA *SEXUAL OFFENCES ACT* 2003 Y EL CONVENIO DE ESTAMBUL. BREVES CRÍTICAS Y CONSIDERACIONES

Lucas O. Maggi[1]

El flagelo de la agresión sexual en todos los entornos de la vida social, incluidas las violencias sexuales cometidas en el ámbito digital es un fenómeno que va en aumento, que a diario encuentra nuevas metodologías. Es por ello que los esfuerzos normativos en pos de paliar los resultados disvaliosos derivados son más que loables.

La presente ley en análisis, tal como surge de su preámbulo, pretende dar respuesta especialmente a las violencias sexuales cometidas en el ámbito digital, lo que comprende la difusión de actos de violencia sexual a través de medios tecnológicos, la pornografía no consentida y la extorsión sexual.

Sin perjuicio del valor de estos esfuerzos normativos, entiendo que la labor del jurista es probar a diario las limitaciones, ventajas y desventajas de un determinado tipo penal. Es por ello que propongo realizar un sucinto análisis de la norma y marcar los aspectos que, en un futuro, creo pueden causar algunos si no varios dolores de cabeza.

En primer lugar, y a fin de evitar controversias, quiero destacar que tengo la íntima convicción de que es adecuado tratar como agresión sexual cualquier conducta sexual que se realice sin consentimiento, en la línea de lo establecido en el artículo 36 del Convenio de Estambul y de lo apuntado por el propio Tribunal Europeo de Derechos Humanos (TEDH). Y es por ello que digo que el análisis de la nueva redacción del art. 178 del CP español no deviene en una mera cuestión doctrinaria, como se verá, nos encontramos con el conflicto de que con la nueva redacción no es suficientemente clara, social y juridicamente, la distinción entre modalidades de agresión sexual y de abuso sexual. Por ejemplo, en un caso de utilización de un perfil falso con fines de manipular el consentimiento de una persona a fin de conseguir su voluntad a favor de un encuentro sexual, podría con esta redacción quedar encuadrado en la figura se produzca o no el encuentro, dado que en estos casos la conducta puede ser igualmente lesiva desde el momento en que se tiende a romper el consentimiento, independientemente del resultado final. Entendemos que el objeto de la teoría del delito es formular reglas generales que, sin afectar las particularidades de cada caso, sirvan para *imputar cualquier hecho punible* a determinadas personas a las que se atribuye responsabilidad por haberlo cometido. Y si bien esa pretensión sólo es posible si más allá de sus diferencias, necesariamente todos los delitos reúnen iguales características, es decir los mismos elementos esenciales. Ello permite al juzgador graduar la gravedad de la conducta partiendo desde los medios empleados hasta el resultado conseguido. Convirtiéndose en una útil herramienta a favor del principio de proporcionalidad.

[1] Staff LawCedic. Abogado, miembro titular del estudio MAGGI & Asoc. Abogados. Diplomado en Cibercrimen y Tecnologías Aplicadas a la Investigación por la Universidad Austral Argentina y por la Universidad Abat Oliba C.E.U. (Barcelona). Ha realizado numerosos cursos de grado y posgrado logrando titulaciones en Universidades de prestigio Internacional, incluyendo un Certified of Achivement in CONTRACT LAW emitido por la HARVARD LAW SCHOOL de los EE.UU.

Como vemos, y en marco de lo que nos compete, la nueva redacción puede resultar útil para seguir orgánicamente los lineamientos establecidos jurisprudencialmente, a saber la STS n.º 447/2021, del 26 de mayo, subraya, entre otras cosas, que: "Los elementos diferenciales entre la ciber violencia o la ciber intimidación respecto a la violencia o a la intimidación ejercida sobre la víctima en un escenario ofensivo de continuidad o proximidad física, no son suficientes para generar categorías normativas de intimidación distintas que impidan la subsunción de tales conductas en los tipos de agresión sexual", así como que "si bien el Código Penal renuncia a definir la intimidación como fórmula de acción, ello no quiere decir que no puedan ni deban extraerse rasgos constitutivos y comunes que permitan delimitarla de cualquier otra fórmula expresiva con intención conminatoria"[2].

Sin perjuicio de lo antedicho, la nueva redacción del 178 CP y el llamado "Yes Model" merecen algunas consideraciones a saber:
CÓDIGO PENAL ESPAÑOL - ART 178 : *Será castigado con la pena de prisión de uno a cuatro años, como reo de agresión sexual, el que realice cualquier acto que atente contra la libertad sexual de otra persona sin su consentimiento. Se entenderá que no hay consentimiento cuando no se haya manifestado libremente mediante actos que, en atención a las circunstancias del caso, expresen de manera clara e inequívoca la voluntad de la persona. 2. A los efectos del apartado anterior, se consideran en todo caso agresión sexual los actos de contenido sexual que se realicen empleando violencia, intimidación o abuso de una situación de superioridad o de vulnerabilidad de la víctima, así como los que se ejecuten sobre personas que se hallen privadas de sentido o de cuya situación mental se abusare y los que se realicen cuando la víctima tenga anulada por cualquier causa su voluntad"*.

Que al menos desde la lectura técnica del artículo, y sin contar a la fecha, por su novedad, con jurisprudencia que nos otorgue un horizonte interpretativo, me atrevo a decir que la técnica legislativa empleada no es la más feliz a los ojos operadores jurídicos. En primer lugar, porque incurre en un alto grado de redundancia, pues si hubiese consentimiento no habría atentado a la libertad sexual. Entiendo que fue la forma que el legislador encontró para dejar bien en claro que la norma se encuadra en el ***"Yes Model"***, pero la redacción no es la mejor.

En segundo lugar, también resulta llamativa la redacción en cuanto "cualquier acto que atente contra la libertad sexual" dado que en rigor técnico permite incluir como conducta disvaliosa actos que impidan manifestaciones de la libertad sexual desde una perspectiva positiva, a saber una madre que impide que su hija menor de edad se conecte a sitios de oferta sexual o donde pueden mantenerse conversaciones de índole sexual, o el padre de una niña con alguna discapacidad o patología médica le prohíba a su hija tener relaciones sin protección con alguna persona, o llevándolo al extremo casuístico imaginemos a un propietario de una casa que encuentra a dos de sus invitados teniendo relaciones sexuales en uno de las habitaciones de la casa, y los obliga a terminar con el coito. Entiendo que esta no es la voluntad del legislador y si así lo fuera sería contraria al principio de ultima ratio del Derecho penal, así como al principio de necesidad. Bien es sabido que el concepto de delito debe ser además funcional con la misión del derecho penal y con los instrumentos de que dispone, lo que obliga a ponderar los efectos sociales que produce cada proposición metodológica. En otras palabras, la consecuencia de cada proposición debe ser plausible, desde perspectivas de política criminal[3]. Y es por ello que si bien la aplicación de un determinado tipo penal debe deducirse de la ley, dicha aplicación debe tender a generar consecuencias político criminales útiles para la sociedad. Ello porque la norma debe tener una finalidad social y actuar como factor de cambio, impulsando su permanente evolución[4]. Siguiendo estos lineamientos la redacción tampoco resulta de lo más feliz.

Por todo ello, en mi opinión es preferible definir el tipo penal de la agresión a través de sus rasgos básicos sin aclaraciones que resulten vagas. Si la conducta prohibida es la de aquel que impone actos de significado sexual en desmedro de la voluntad de otra persona o realiza actos con intención de llegar a un resultado sexual en desprecio de la voluntad de otra persona, debería ser así de sencilla su definición.

2 STS 447/21 https://www.poderjudicial.es/search/AN/openDocument/efe79b54d612084a/20210224
3 Roxin, Claus, Política criminal y sistema del derecho penal, trad. por Francisco Muñoz Conde, Bosch, Barcelona, 1972, ps. 15 y ss.
4 Righi Derecho Penal: Parte General. 2a Ed. Actualizada IV - Teoría del delito. Método.

De esta forma el principio de proporcionalidad también se vería respetado porque el juez tendría la herramienta para juzgar las apariencias de consentimiento, como ejemplo el llamado prevaliamiento, o todo tipo de superioridad o presión del agresor en la situación, hasta llegar a los casos más graves donde se doblega la voluntad contraria de la víctima mediante violencia o intimidación, y así también utilizar la figura cuando nos encontremos con indicios de aprovechamiento de la imposibilidad de la otra persona de manifestar su consentimiento. Eso es posible porque en todos los casos nos encontramos con el rasgo típico diferencial de la figura, el consentimiento viciado o su ausencia[5].

Asimismo, nuevamente nos encontramos con complicaciones para la aplicación de la definición de consentimiento, ello respecto a crítica sobre la certeza del concepto, dado que la actual definición cae en la misma problemática que el modelo "No means No", no se establece un marco que limite las manifestaciones consideradas como afirmativas para la realización de actos sexuales. Veamos, "Se entenderá que no hay consentimiento cuando no se haya manifestado libremente mediante actos que, en atención a las circunstancias del caso, expresen de manera clara e inequívoca la voluntad de la persona", el problema radica en que la norma no define el consentimiento, lo que define es cuando no lo hay.

En vez de utilizar fórmulas negativas podría haberse recurrido a una definición positiva del consentimiento con fines interpretativos dentro de la norma, *con el fin de evitar las dudas que pudieran derivar de la utilización de una doble negación en castellano, como también la confusión que esa doble negación pudiera generar acerca del modelo de consentimiento* (de la opinión de Consejo de Europa)[6].

Cuando hablamos positivamente de consentimiento, hablamos de una disposición mental de querer hacer algo, de desear realizar una conducta, que en el ámbito de las relaciones sexuales se refiere a la voluntad de realizar una interacción sexual libre de coacciones y amenazas, ya que es una muestra más de la autonomía que tenemos los seres humanos por el hecho de serlo y que tiene el poder de cambiar situaciones y realidades[7]. Definición típica de la que tenemos varios ejemplos y que tranquilamente podrían haberse orientado a la línea del artículo 36.2 del Convenio de Estambul: "El consentimiento debe prestarse voluntariamente como manifestación del libre arbitrio de la persona considerado en el contexto de las condiciones circundantes". En la misma línea la *Sexual Offences Act* 2003 aplicable en Inglaterra y Gales, en la que la prestación del consentimiento se define en sentido positivo con referencia a la libertad y a la capacidad de la persona ("74. For the purposes of this Part, a person consents if he agrees by choice, and has the freedom and capacity to make that choice")[8].

En consecuencia y, no siendo el objetivo de este trabajo dar más que una consideración y una apreciación técnica respecto a la operatividad de una norma y sus posibles consecuencias, debo decir, a modo de sucinta conclusión, que entiendo que la discusión aún no está zanjada, será importante la colaboración de todos los operadores del derecho, y tarea doctrinaria y jurisprudencial obligada, el establecer el correcto alcance de aplicación de la norma, y será el tiempo y sus resultados quienes juzgarán si el modelo resultaba correcto.

5 A mayor abundamiento ver dictamen del Consejo de Estado Español del 10/06/21 Exp.393/21.
6 Consejo de Estado Español del 10/06/21 Exp.393/21.
7 HURD, Heidi, *The moral magic of consent*, Cambridge University Press, Legal Theory, 2, pp. 121- 146. 1996, United States of America.
8 Sexual Offence act. definitive guideline. Govern of UK:
https://www.sentencingcouncil.org.uk/wp-content/uploads/Sexual-offences-definitive-guideline-Web.pdf

OCEDIC

OBSERVATORIO DE CIBERCRIMEN Y EVIDENCIA DIGITAL
EN INVESTIGACIONES CRIMINALES

DIRECTORA DANIELA DUPUY

SUBDIRECTORA CATALINA NEME

LAWCEDIC

TEAM LEADER: DENISE GROSS

EDICIÓN: NATALIA PEREYRA - MARÍA LOURDES PETRECOLA - ANA ZOLEZZI MIR

COLABORADORES: ANTONELLA BENTIN - JUAN PABLO ANDUEZA
CAMILA JULIETA LANZILLOTTA - LUCAS MOYANO - FÉLIX FABIÁN ESPINOZA VALENCIA
LUCAS MAGGI - MÓNICA FERNÁNDEZ CAMPERO - RICARDO DANIEL CARREÑO

DISEÑO: LEONARDO SMITSAART

DISEÑO WEB: MATÍAS NICOLÁS GARCÍA

OCEDIC.COM

ocedic@austral.edu.ar

UNIVERSIDAD AUSTRAL | DERECHO

Cerrito 1250 (C1010AAZ) - CABA - Argentina