Delitos, prueba y evidencia digital

Leopoldo Sebastián M. GÓMEZ

Abogado y Licenciado en Ciencias de la Computación
Perito Informático Oficial - Poder Judicial del Neuquén
sebastian.gomez@jusneuquen.gov.ar

Abstract. Homicidios, abusos sexuales y pornografía infantil son algunos de los delitos en los que la evidencia digital puede ser crucial para la búsqueda de la verdad. Es por ello que es oportuno tratar aspectos jurídicos sobre la actividad pericial, así como también otros lineamientos para la admisibilidad y relevancia de la evidencia digital. Mediante el análisis de precedentes jurisprudenciales actuales se promueve la utilización de la evidencia digital como un elemento probatorio de singular importancia para las investigaciones judiciales. Referido al derecho penal sustantivo, se resaltan criterios actuales para la determinación de la competencia en causas judiciales sobre venta de CDs y DVDs apócrifos, finalizando con una exposición de aspectos controvertidos en la práctica forense para la identificación de imágenes de pornografía infantil.

Keywords: delitos, nuevas tecnologías, prueba, evidencia digital, Ley 26.388

1 Introducción

Las garantías del art. 18 de la C.N. presupone la posibilidad de traer al conocimiento del juez las pruebas necesarias para el esclarecimiento de la verdad [1]. Principia el desarrollo de la temática considerar el principio de libertad de la prueba, en concordancia con los códigos de rito penales de Argentina y la jurisprudencia consagrada reiteradamente con la CSJN a la cabeza, por el cual "en el proceso penal todo puede ser probado por cualquier medio" en base a los principios de investigación integral y la garantía constitucional de la defensa en juicio que se dirigen en pos de la verdad jurídica objetiva [2].

Sin perjuicio de las posturas doctrinarias sobre la enumeración taxativa o enunciativa de los medios probatorios, el verdadero problema radica en las fuentes de evidencia digital. La aparición de nuevos elementos tecnológicos –computadoras, dispositivos de almacenamiento magnéticos, cámaras digitales, telefonía celular- y otros como Internet, el correo electrónico y la firma digital revelan la inusitada expansión de las fuentes de prueba [3].

Bajo esta premisa resulta de interés explicitar la modalidad por la cual se introducen dichos elementos probatorios por los medios regulados por la ley. Estamos en el ámbito de la pericia informática. Es importante destacar que la pericia está dirigida a descubrir o valorar un elemento de prueba siempre que para ello sea

necesario o conveniente tener conocimientos especiales de alguna ciencia, arte o técnica (art. 253 CPPN), y se concretará en una conclusión, fruto de un juicio realizado al amparo de esos conocimientos especiales. En cuanto a los informes técnicos policiales, corresponde indicar que podrían ser ordenados "si hubiera peligro de que cualquier demora comprometa el éxito de la investigación" (art. 184 inc° 4, CPPN), sin exigir a quienes los lleven a cabo títulos especiales.

Clariá Olmedo [4] sostiene que el perito es un particular que desempeña en el proceso un servicio público; es pasible de responsabilidad penal y civil y procesalmente controlado. De aquí que por regla deba ser titulado en la materia que se trata o idóneo reconocido si la aquella no está reglamentada.

En palabras de Caferatta Nores [5], la práctica, con el apoyo de la jurisprudencia, ha ampliado incorrectamente el campo de los informes técnicos policiales, siendo importante recordar la naturaleza descriptiva de estos últimos. Si el informe técnico policial excede este ámbito, será necesario realizar una pericia en sentido propio, a la cual aquél no podrá sustituir. Asimismo, una intervención inapropiada resultaría totalmente perjudicial para la admisibilidad del elemento probatorio, dado que la evidencia digital es frágil y susceptible de ser alterada si no se toman los recaudos necesarios. Es por ello que más allá de la distinción entre los elementos formales de ambos informes, debe considerarse con especial atención las cuestiones atinentes a la contaminación de la prueba, la idoneidad necesaria para la pericia, y la amplitud y alcance de la actuación profesional del perito informático, que va más allá de las operaciones técnicas sobre la evidencia digital.

Por otra parte, es imprescindible propiciar la adopción de lineamientos que permitan una correcta definición del alcance de los servicios profesionales de informática forense, que contribuyan a profundizar los resguardos en la cadena de custodia de la prueba y expliciten la modalidad del trabajo pericial para una mejor adecuación de los requerimientos judiciales. En el ámbito judicial, la formalización y aprobación de un documento institucional con carácter reglamentario orienta al logro de este objetivo [6].

Con frecuencia los esfuerzos profesionales para elevar la calidad del servicio pericial ofrecido a los operadores judiciales se ven opacados por la falta de apoyo institucional. Los operadores judiciales deben procurar una oportuna actualización de conocimientos para poder comprender el impacto que han provocado los avances tecnológicos en la sociedad y con ello el crecimiento sostenido que tendrán las nuevas fuentes de prueba digital. Se requiere un esfuerzo intelectual no solamente en cuestiones de derecho penal sustantivo, sino también en los aspectos de derecho penal adjetivo atinentes a la relación entre la investigación judicial y las nuevas tecnologías.

Sigue siendo habitual encontrar ambigüedad en los requerimientos judiciales y esporádicamente se presentan otras actividades operativas elementales enmascaradas como "puntos de pericia"[1]. En estos casos, el perito se encuentra en una difícil

[1] En cuanto a la procedencia de la pericia, no se debe requerir la intervención del perito para la realización de meras comprobaciones materiales que pueden ser llevadas a cabo por cualquier persona, cuando dentro del criterio de la cultura normal, o cultura general, se puede hallar la

situación de desgaste personal al intentar adecuar los requerimientos de un operador judicial inexperto a los servicios periciales ofrecidos, en función de la experticia y las posibilidades técnicas y humanas. Las fallas en la comprensión del trabajo forense se producen principalmente por el desconocimiento de esta nueva especialidad y la falta de formalización e institucionalización de los servicios periciales. Resulta oportuno recordar que el perito, por encargo del juez, actúa como órgano imparcial o auxiliar de la Justicia que aporta la prueba. Sin embargo, ser auxiliar no significa ser subalterno del juez, ni sujeto del órgano jurisdiccional, sino un tercero que colabora en la investigación de los hechos, aportando el auxilio de su ciencia o de su técnica para su verificación total o parcial, cuando tienen especiales características técnicas, científicas o artísticas.

2 Consideraciones jurídicas sobre la prueba digital

En un acertado enfoque hacia las nuevas tendencias procesales y la tecnología informática, Salt [7] manifiesta la importancia de regular en los Códigos Procesales Penales normas especiales destinadas tanto a la investigación de los delitos informáticos como así también a la obtención de evidencia digital destinada a la acreditación de los extremos fácticos de los demás tipos penales. Riquert [8] observa que el camino a seguir habrá de ser el dotar a los órganos encargados de la persecución pública de cuerpos especializados que estén a la altura de los desafíos técnico-periciales que se debe afrontar y capacitando a los fiscales para que presenten el caso a juzgar con solidez, con una adecuada valoración de la prueba directa e indiciaria que se pueda obtener, sin resignar principios basales de un sistema procesal acusatorio, que es el que corresponde a un Estado de Derecho. En esta línea de pensamiento, y considerando los tiempos dilatados para llevar adelante las reformas procesales, es útil y conveniente iniciar la formalización de protocolos de actuación para facilitar el trabajo interdisciplinario entre operadores judiciales y especialistas en disciplinas forenses. En la actualidad existen algunos documentos reglamentarios, sin embargo en materia de pericias informáticas aún se requieren grandes esfuerzos para lograr formalizar el alcance y modalidad de las actividades forenses[2].

Párrafo aparte merece el tratamiento otorgado a las fuentes de evidencia digital a la luz de la reforma del Código Penal por la Ley 26.388. Si bien el legislador ha

---

regla o el criterio para resolver la cuestión; es decir, cuando pueda solucionársela mediante los conocimientos básicos de cualquier hombre culto (Cfr. Cafferata Nores, J., *La Prueba*..., ob cit. p 68).

[2] En el Poder Judicial del Neuquén se elaboró un documento formal titulado "Catálogo de Servicios y Protocolo de Actuación para Pericias Informáticas", siendo esencial y oportuno que dicho texto tuviese carácter prescriptivo para facilitar la interacción profesional. Sin perjuicio que su elaboración data desde hace varios años y de haber propiciado su aprobación mediante un Acuerdo administrativo en reiteradas oportunidades, por cuestiones de retardo en la gestión administrativa el documento sólo ha podido ser distribuido y llevado a conocimiento de los operadores judiciales en carácter informativo.

sabido interpretar la importancia de la cadena de custodia de los elementos probatorios[3], la realidad de la práctica judicial dista mucho del delicado tratamiento que debería darse a las fuentes de evidencia digital. Esto no sucede necesariamente por falta de recursos materiales[4], sino porque se minimiza el riesgo de alteración de la prueba por falta de capacitación o bien simplemente por desidia del operador judicial. Más allá de los avances en materia de seguridad, se requieren operadores judiciales y de las fuerzas de la ley debidamente capacitados en esta temática, con el objeto de lograr el fin deseado. La experiencia indica que aún luego de varios años de haber sido implementadas las medidas de seguridad apropiadas, siempre puede subsistir algún que otro inconveniente provocado por la ausencia de un control responsable en el manejo de las fuentes de evidencia digital. Otra cuestión crítica a considerar es la falta de depósitos adecuados para el resguardo de este tipo de material probatorio, en función de los cuidados especiales y espacio físico que requieren los elementos tecnológicos, siendo habitual que las típicas oficinas de secuestros no alcancen los requisitos mínimos para garantizar la correcta preservación de las fuentes de evidencia digital.

En cuanto a la relevancia de la prueba digital, baste decir que en los precedentes jurisprudenciales se reflejan o confirman muchos de los resultados de la actividad pericial informática. A título ejemplificativo, en una investigación judicial por abuso sexual cometido prima facie por un ginecólogo y en la que se había dispuesto el sobreseimiento del imputado, los apoderados de la parte querellante interpusieron un recurso de apelación. Durante la investigación judicial, la identificación y extracción de fotografías digitales con desnudos localizadas en el disco rígido de la notebook personal del ginecólogo y que fueran aportadas como resultado de la pericia informática, constituyó un elemento esencial para posibilitar posteriormente al médico forense la emisión de un dictamen afirmando la existencia de prácticas médicas abusivas. La Cámara de Apelaciones en lo Criminal con competencia provincial de Neuquén -por unanimidad- revocó el sobreseimiento. La R.I. Nº 545/09, 11/12/09, expresa en los considerandos: "…hay otros elementos más allá de los dichos de quien viene figurando como víctima, por ejemplo la obtención de algunos que no tienen que ver con la práctica médica (fotos extraídas en el consultorio)…" "…Completa el segundo agravio la mención a la falta de ponderación de algunos

---

[3] Art. 255 C.P.: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

[4] Desde el año 2008 en el Poder Judicial del Neuquén se proveen etiquetas de seguridad a todos los organismos del fuero penal. Dichos elementos deben ser entregados al personal policial al momento de entregar la orden de allanamiento para su utilización sobre los secuestros de tecnología informática. Al resguardar el material probatorio con estos precintos se garantiza la cadena de custodia desde el inicio del procedimiento judicial.

elementos relevantes reunidos. En este sentido, se menciona que el a quo no considera de manera concreta la colección de fotos de mujeres desnudas secuestradas, que es reveladora de una práctica profesional abusiva…" "…la extracción de fotografías a la testigo M.N.S., absolutamente desnuda, presuntamente para hacer una interconsulta que nunca se concretó…". Atendiendo a los fundamentos vertidos por el tribunal de alzada se puede apreciar la incidencia y relevancia que comienza a tener la evidencia digital en las investigaciones judiciales.

Por otro lado, en materia de casuística referida a infracciones a la Ley 11.723, entiendo que no amerita profundizar en el análisis jurídico del concurso ideal de delitos por infracción al artículo 31 inc. d) de la ley 22.362 y el art. 72 bis inc d) de la ley 11.723 sobre el cual ya existe abundante doctrina del Alto Tribunal[5]. Sin embargo en mi opinión, es dable aclarar que previo a la calificación legal de un caso con CDs o DVDs apócrifos, lo determinante es discernir si los elementos secuestrados que constituyen la prueba tienen entidad suficiente como para producir el engaño y la afectación de derechos marcarios que la ley 22.362 protege. En esta línea de pensamiento, existen precedentes jurisprudenciales con criterios coincidentes con la posición adoptada[6]. En igual sentido se ha pronunciado la Cámara Federal en cuanto a la venta de CDs apócrifos a través de un sitio de Internet[7]. A la fecha de la elaboración del presente trabajo, la jurisprudencia argentina continúa acordando

---

[5] "....corresponde a la justicia federal más allá que la infracción a la ley 11.723 sea ajena a su conocimiento, continuar la sustanciación de la causa, en razón de que el caso resulta aprehendido por dos disposiciones legales -leyes 22.362 y 11.723- que concurrirían en forma ideal, pues ambas habrían sido cometidas simultáneamente y mediante una única conducta (Fallos 323:169,870 y 2232)..." (conf. C.S.J.N. en causa "Araujo, Oscar", fallo del 11.03.08, entre muchos otros; v. en el mismo sentido esta Sala in re "Pruzzo, Eugenia a/su dcia.", expte. n° 4880, del 6.11.08).

[6] "Si las láminas de los discos compactos secuestrados -que serían reproducciones ilegítimas de sus originales en infracción a la ley 11.723-, resultan apócrifas, no aparece violada la ley de marcas y designaciones –ley n°22.362-, si tales láminas resultan imitaciones burdas, manifiestamente reconocibles a simple vista, insusceptible de reproducir confusión en los consumidores. Así, se debe disponer que continúen las actuaciones en conocimiento de la justicia de instrucción" (CNCC, Sala IV, cn° 20.603, "Aceval, Eduardo", rta.2/12/04).

[7] En esta causa, el imputado presuntamente vendía a través del sitio www.mercadolibre.com.ar CDs que grababa en su misma PC. En su domicilio se secuestraron 44 ejemplares de éstos productos apócrifos, una CPU con copiadora de CDs, que contenía en su memoria 574 archivos de mp3, y programas para su grabación. Además constaban en la causa algunos e-mails que el imputado intercambió con el denunciante, una compradora de los CDs. Esos correos electrónicos, para los camaristas, resultaron "demostrativos de las características de la operatoria de venta". Asimismo los integrantes de la sala II de la Cámara Federal destacaron que "los discos compactos presentaban notorias diferencias con los genuinos no sólo en el estuche exterior, sino también en el producto en sí mismo, por cuanto los discos propiamente dichos ostentan sólo la marca de los denominados "vírgenes" (CNCC, Sala II, "Krohn, Marcelo s/Infracción Ley 22.362", 30/12/04).

competencia a la Justicia ordinaria para aquellos casos de venta de CDs y DVDs en los que sea notoria la imitación de las carátulas originales[8].

Referido a homicidios, robos u otros delitos convencionales, es indiscutible el aporte que puede brindar la evidencia digital para el esclarecimiento del hecho investigado a partir del análisis de teléfonos celulares y todo otro elemento tecnológico (cámaras digitales, pendrives, etc.). Mediante agendas de contactos es posible que el operador judicial esclarezca la identificación de personas y redes sociales, establezca una cronología de sucesos en función de registros de llamadas, y correlacione otros acontecimientos a partir de mensajes de texto e imágenes digitales. A las clásicas posibilidades de triangulación de un teléfono celular mediante información técnica obtenida del proveedor de servicios de comunicaciones, se suma la facilidad de geolocalización que ofrece la tecnología GPS, a través de información técnica o metadatos extraídos directamente desde los dispositivos tecnológicos.

En cuanto a la producción, ofrecimiento y distribución de pornografía infantil, es acertada la reflexión de Palazzi [9] sobre la necesidad de flexibilizar nuestros criterios ancestrales en materia de soberanía, territorialidad y competencia del juez penal a fin de traer mayor eficiencia y justicia en los casos de delitos informáticos. Asimismo, está demostrada la dificultad que entraña resolver cuándo hay "finalidad inequívoca de distribución o de comercialización" conforme lo previsto por el segundo párrafo del art. 128 CP[9].

Sin ahondar en la problemática que introduce Internet para el rastreo de redes de pedofilia, se suscitan varios inconvenientes al efectuar pericias informáticas tendientes a la localización de imágenes de pornografía infantil sobre dispositivos tecnológicos. En primer lugar, el constante aumento en la capacidad de los medios de almacenamiento permite que el usuario acumule una gran cantidad de fotografías digitales sin tener que preocuparse por el espacio ocupado. En la actualidad sigue siendo imposible realizar en forma manual un examen exhaustivo de aquellos archivos que contienen imágenes, y debe procurarse recurrir a software forense especializado para efectuar reducciones automáticas en el espacio de búsqueda de evidencia digital con el objeto de determinar contenidos ilícitos.

---

[8] CNCC, "Pérez González, Luis Damián s/competencia", Expte. 43.313, 17/11/09, consultado en http://www.cij.gov.ar/buscador-de-fallos.html

[9] Art.128 C.P.: Será reprimido com prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explíctas en el que participaren dichos menores. Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años.

Finalmente, resulta evidente la dificultad que se le presenta al perito informático en su intento de identificar o filtrar imágenes asociadas al delito tipificado por el art. 128 C.P. respecto a la edad de las personas. En concordancia con lo referido, Carbone [10] sostiene que "el aspecto más controvertido sin dudas, será el de la edad, y así no podría cometerse el delito si las imágenes de actividades sexuales explícitas o de genitales que en apariencia fueran de un menor, pertenecieran a un mayor de 18 años; y por el contrario, podría cometerlo quien llevara adelante alguno de los actos típicos con imágenes en apariencia de un mayor pero que pertenezcan en la realidad a un menor aunque en ese caso cabría eventualmente la invocación de error que podría ser de tipo (o de hecho)-, cabiendo además preguntarse acerca de si sería viable la posibilidad de dolo eventual, lo que en nuestro modo de ver resultaría un exceso, tratándose de un delito de peligro abstracto". Abordando esta cuestión desde la práctica pericial, ha de considerarse que un experto en informática forense carece de conocimientos científicos sobre anatomía, los que en muchos casos resultan necesarios para aseverar indubitablemente que los hallazgos de fotografías digitales de desnudos o sexo explícito corresponden a pornografía infantil. Es por ello que, si de las imágenes resultantes de la pericia informática no puede ser definida la edad de las personas con los conocimientos de cualquier persona culta, es conveniente someter la evidencia digital obtenida ante un especialista en medicina forense para que dictamine sobre este punto.

Una cuestión conexa a este tipo de pericias está vinculada a la exposición del especialista a las imágenes de pornografía. Si bien en los últimos años se han comprobado avances en la ciencia informática y mejoras en los algoritmos para detección de imágenes con contenido sexual, todavía no existe una total automatización de estas tareas periciales y se debe recurrir en última instancia a la inspección visual para convalidar los hallazgos digitales. El trabajo continuo sobre casos de pedofilia y otros asociados con material pornográfico es perjudicial, provoca situaciones de estrés, afecta a la moral y puede producir daños psicológicos. Han comenzado a surgir herramientas forenses especializadas que aplican filtros Blur –también conocido como desenfoque gaussiano- para intentar mitigar este tipo de situaciones agraviantes.

3 Conclusiones

Con una perspectiva cotidiana del quehacer pericial se han abordado aspectos jurídicos y criterios profesionales que permitirán cohesionar la investigación de delitos convencionales o "informáticos" con los elementos de prueba obtenidos desde nuevas fuentes de evidencia digital.

Se analizó la problemática que presentan las nuevas tecnologías en su interrelación con el derecho penal, así como también con el derecho procesal penal. En un primer enfoque orientado hacia aspectos procesales, y ante el inusitado alcance que la práctica judicial suele otorgar a los llamados informes técnicos policiales, se ha presentado la oportunidad de plantear una reivindicación de los dictámenes periciales sobre aquellos. En materia de pericias informáticas, esta distinción requiere avanzar

más allá de los elementos formales, haciendo especial énfasis en la metodología y técnicas forenses aplicadas para evitar la contaminación de la prueba, y considerando aspectos de idoneidad, amplitud y alcance de la actuación profesional del perito informático.

Actualmente existe una carencia de normas especiales en los Códigos Procesales para la investigación de delitos informáticos u otros en los que deba obtenerse prueba mediante evidencia digital, así como una insuficiente capacitación de los operadores judiciales en este área de especialidad. Ante esta situación desfavorable, se plantea como remedio paliativo la formalización de protocolos de actuación dentro del ámbito judicial para mejorar la interacción profesional.

En cuanto a la admisibilidad de la prueba, la cadena de custodia sigue siendo uno de los aspectos críticos para el éxito de la investigación judicial. Atendiendo a ello, los operadores judiciales y personal policial han de tomar los recaudos necesarios en el manejo de fuentes de evidencia digital, atendiendo a los resguardos mínimos a fin de que no se frustre la investigación por contaminación o sustracción de los elementos probatorios. Aunque sin mayores cambios en lo referido al art. 255 del Código Penal, es dable recordar que la reforma introducida por la ley 26.388 mantiene vigente la punibilidad para la sustracción, alteración, ocultamiento, destrucción o inutilización en todo o en parte de los objetos destinados a servir de prueba ante autoridad competente.

En referencia a la casuística con CDs o DVDs apócrifos parece razonable determinar, en un análisis previo a la calificación legal, si la prueba es apta como para producir el engaño y la afectación de derechos marcarios. Si ello no ocurriere –y en un todo de acuerdo con la jurisprudencia- corresponderá otorgar competencia a la Justicia ordinaria quien deberá investigar una posible infracción a la ley 11.723.

Sigue sorprendiendo la relevancia que toma la evidencia digital en delitos tradicionales como homicidios, robos y abusos sexuales. Los elementos de prueba obtenidos de la pericia informática resultan en muchos casos esenciales para el esclarecimiento del hecho investigado. Es de esperar que el operador judicial comprenda y valore las posibilidades periciales que ofrecen los elementos tecnológicos que están al alcance de la población, con especial énfasis en los dispositivos de telefonía celular.

Finalmente se han expuesto los aspectos críticos de la actividad pericial informática en casos por infracción al art. 128 del Código Penal. Si bien se ha comenzado a trabajar con software forense para la detección de imágenes con contenido sexual, la imposibilidad de reconocimiento automático de imágenes de pornografía infantil conlleva al especialista a la utilización de técnicas ad-hoc y filtros sobre imágenes, en un esfuerzo por mitigar los efectos psicológicos adversos que pueden resultar del trabajo con este tipo de material. Referido al problema que plantea la determinación de la edad de una persona en una imagen fotográfica, se plantea como conveniente someter la evidencia digital obtenida ante un especialista en medicina forense para que dictamine sobre este punto.

Tengo la firme convicción que los criterios y lineamientos presentados sobre delitos, prueba y evidencia digital serán bien recibidos por todos los operadores del servicio de Justicia.

Referencias

1. Bidart Campos, G., "Derecho Constitucional", t. II, p.486, Ediar, Bs. As., (1966)
2. Clariá Olmedo, J., "Tratado de Derecho Procesal Penal", t. V., p.33, Ediar, Bs.As., (1966)
3. Carbone, C., "Prueba: Cuestiones modernas", Dir. Morello, A., p.126, La Ley, (2007)
4. Clariá Olmedo, J., "Derecho Procesal Penal", actualizado por Chiara Díaz, C., t. II, p.320, Rubinzal – Culzoni Editores, (2001)
5. Cafferata Nores, J., "La prueba en el proceso penal", p.101, Lexis Nexis, (2008)
6. Gómez, L., "El Protocolo de Actuación para Peritajes Informáticos en el ámbito judicial", Revista de Derecho y Nuevas Tecnologías, http://www.rdynt.com.ar, y Simposio Argentino de Informática y Derecho, JAIIO, Santa Fe, Argentina, Septiembre, (2008)
7. Salt, M., "Tecnología informática: un nuevo desafío para el Derecho Procesal Penal?", XXV Congreso Nacional de Derecho Procesal, http://www.procesal2009bsas.com.ar, (2009)
8. Riquert, M., "Algo más sobre la legislación contra la delincuencia informática en Mercosur: a propósito de la modificación al Código Penal argentino por ley 26.388", Alfa-Redi, Agosto, (2008)
9. Palazzi, P., "Los Delitos Informáticos en el Código Penal – Análisis de la ley 26.388", Abeledo Perrot, (2009)
10. Carbone, D., "Comentario a la ley de delitos informáticos. 26.388. Nuevos delitos-viejos delitos", Microjuris, (2008)