eNAC

The Cybex Initiative | e-NEWSLETTER EN LA LUCHA CONTRA EL CIBERCRIMEN

www.cybex.es
Nº4 · OCTUBRE · 2009

LEGAL

Juan Carlos Ortiz realiza un análisis del Remote Forensic Software como instrumento para la investigación policial y judicial en la lucha contra el terrorismo, tal y como ha sido recogido en la Ley alemana de Defensa contra los Peligros del Terrorismo Internacional.

PROTECCIÓN DE DATOS

"¿Cómo al tratar datos de carácter personal puedo estar impactando o incidiendo en la privacidad de las personas?" un artículo de Ramón Miralles de la Agencia Catalana de Protección de Datos.

TÉCNICA

José Duart, experto en ingeniería inversa y análisis forense, hace una aproximación a las técnicas anti forenses en NTFS.

CUERPOS Y FUERZAS DE SEGURIDAD

La disciplina de la técnica forense aplicada a la ciberdelincuencia engloba diversas funciones con distintos grados de responsabilidad. David Childs de la Oficina de Defensa del Consumidor de North Yorkshire habla sobre los diferentes roles involucrados en una investigación.

INSTITUCIONAL

El artículo de Radomír Janský y Ruben Lombaert de la Comisión Europea nos acerca a las estratégias de la Comisión en cooperación con los Estados Miembros e Instituciones Internacionales.

JURISPRUDENCIA

Los casos resumidos en esta publicación tratan sobre el modo en que las personas utilizan dispositivos digitales para realizar negocios, y el modo en que los requisitos normativos de forma impuestos por los políticos se ignoran o se desconocen (probablemente, el verdadero motivo sea este último).

EVENTOS

Selección de conferencias de interés para cuerpos y fuerzas de seguridad, abogados, fiscales, especialistas en análisis forense de dispositivos digitales, directores de recursos humanos, jueces y cualquier persona que trate con prueba electrónica y/o trabaje en la prevención del cibercrimen.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

eNAC
e-NEWSLETTER EN LA LUCHA CONTRA EL CYBERCRIMEN
www.cybex.es
Nº4 · OCTUBRE · 2009

Índice

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

eNAC

e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME

Queridos lectores,

Nos complace compartir con vosotros la incorporación de un nuevo Editor al equipo del ENAC: Esther George, Consejera política Senior y Abogada del Estado en el 'Crown Prosecution Service', el Ministerio Fiscal de Reino Unido.

Esther George será co-editora de la sección legal del ENAC junto con Pedro Verdelho.

Esther George es Consejera política Senior y Abogada del Estado en el 'Crown Prosecution Service (CPS) HQ Policy Directorate'. Está especializada en crímenes cometidos a través de internet y dispositivos electrónicos, prueba electrónica y protección de datos. En Enero de 2002, Esther pasó a ser la directora del proyecto del CPS sobre Delitos Tecnológicos. Ha sido Consejera de fiscales a todos los niveles entre HQ y las oficinas de CPS, cuerpos y fuerzas de seguridad y organismos gubernamentales. Actualmente actúa como consejera de los fiscales en casos de delitos tecnológicos.

Además, Esther está diseñando un programa de formación para fiscales sobre delitos en la propiedad intelectual y su procesamiento. Inició y actualmente forma parte del Global Prosecutors E-Crime Network (Red General de Fiscales sobre Cibercrimen, GPEN), que permite a fiscales especializados en delitos tecnológicos de todo el mundo formarse y beneficiarse al compartir información, experiencias y estrategias, reforzando como resultado la cooperación internacional.

Queremos agradecer a Carmen Lázaro, nuestra co-editora hasta el momento de la sección legal del ENAC, su gran contribución, dedicación y trabajo realizados durante los primeres meses de vida del e-Newsletter.

Finalmente, queremos dar una cálida bienvenida a Esther al equipo!

Sra. FREDESVINDA INSA
Directora de Proyecto
finsa@cybex.es

Sra. MIREIA CASANOVAS
Coordinadora de Proyecto y Editora Jefe
mcasanovas@cybex.es

Cybex
Plaza Cataluña 20, 9ª planta · 08002 · Barcelona · España
tel. +34 93 272 20 41 · fax. +34 93 215 50 72

Ir a la versión inglesa del ENAC

Ir a la versión rusa del ENAC

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

JUAN CARLOS ORTIZ PRADILLO

Profesor de Derecho Procesal en la Universidad de Castilla-La Mancha, España

EL 'REMOTE FORENSIC SOFTWARE' COMO HERRAMIENTA DE INVESTIGACIÓN CONTRA EL TERRORISMO[1]

Juan Carlos Ortiz es Profesor Contratado-Doctor de Derecho Procesal. Facultad de Ciencias Jurídicas de Toledo, Universidad de Castilla-La Mancha.

Investigador invitado en el Instituto de Derecho Procesal (2002, 2003) y de Derecho Penal Europeo e Internacional (2005) de la Universidad de Colonia y en el Instituto MAX-PLANCK de Derecho Penal Comparado e Internacional de Friburgo (2008).

Doctor en Derecho (2005). Premio Extraordinario de Licenciatura (1996-2000).

1. La revolución digital y la lucha contra el terrorismo

La revolución global en el uso de las nuevas tecnologías, amparada en la reducción de los costes para su adquisición y en la facilidad para su manejo, ha permitido que el uso de la informática se encuentre al alcance de cualquier persona, en cualquier momento y en cualquier parte del mundo, lo cual también tiene graves consecuencias cuando son empleadas para la preparación, comisión o difusión de toda clase de ilícitos. La delincuencia informática, y especialmente la cometida a través de Internet, han crecido exponencialmente a la par que el desarrollo de las nuevas tecnologías, y el terrorismo no es ajeno a dicha evolución. Por ello, se ha puesto especial énfasis en la necesidad de evitar que los grupos terroristas puedan valerse de Internet, no sólo para la comunicación entre sus miembros, sino como "*campo de entrenamiento virtual*" en el que divulgar y hacer apología de sus ideales y actos, incitar a la comisión de atentados, difundir instrucciones para fabricar y utilizar explosivos, o para el reclutamiento de activistas[2].

La respuesta de los gobiernos al desafío constituido por el terrorismo internacional, sobre todo tras los atentados cometidos en Nueva York, Bali, Madrid, Londres o Bombay, ha sido la promulgación de una avalancha de reformas legislativas de urgencia en materia antiterrorista caracterizadas por un recorte de las garantías penales y procesales aplicables a los sospechosos de estar relacionados con actividades terroristas, junto con el correlativo otorgamiento de poderes especiales a los distintos servicios de seguridad de los Estados para la investigación y prevención de conductas relacionadas con tales actividades.

[1] El presente artículo se incardina dentro de los resultados del Proyecto I+D+i MICINN DER2008-03378.
[2] Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre de 2008 por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo (DOUE L 330/2, de 9.12.2008).

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

El presente artículo tiene por objeto el análisis del denominado *Remote Forensic Software* como instrumento para la investigación policial y judicial en la lucha contra el terrorismo, tal y como ha sido recogido en una de dichas reformas legislativas en materia antiterrorista: la Ley alemana de Defensa contra los Peligros del Terrorismo Internacional[3], que comprende nuevas medidas de investigación y entre las cuales se encuentra el "acceso remoto y secreto a los equipos informáticos".

2. El uso de las TIC en la investigación policial y judicial

El uso de la informática y de las nuevas tecnologías ha sido ampliamente asumido en la investigación policial, donde cada vez gana mayor peso la utilización de instrumentos electrónicos para la vigilancia de los movimientos de una persona, pero no mediante su percepción sensorial directa (videovigilancia), sino de manera telemática o remota (tecnovigilancia). Más allá de lo conocido como "ciberpatrullaje", podemos citar, como ejemplo, los sistemas informáticos de lectura automática de matrículas, programas de reconocimiento biométrico de los rostros o siluetas de sujetos o de bultos sospechosos, la instalación de balizas de seguimiento a vehículos y embarcaciones, o el uso de la tecnología GPRS o GSM para conocer la ubicación geográfica de un terminal. Pero dicha adaptación a la Era Digital debe ser también recogida en el ámbito judicial, y aprovechar así las nuevas capacidades tecnológicas susceptibles de ser empleadas durante la fase de instrucción para la averiguación y descubrimiento de los delitos y sus responsables, sin perder de vista la observancia de las distintas garantías constitucionales y legales que protegen a los ciudadanos frente a una injerencia desproporcionada en el ámbito de sus derechos más esenciales.

Un claro ejemplo lo encontramos en la práctica de llevar a cabo inspecciones del disco duro de los equipos informáticos como medida de investigación óptima para la obtención de las evidencias de cualquier clase de delito. Dado que los distintos dispositivos electrónicos e informáticos que tenemos en nuestros hogares y oficinas permiten almacenar, en múltiples formatos, una ingente cantidad de información, resulta cada vez más frecuente que, cuando se efectúa un registro domiciliario, las autoridades encargadas de la investigación criminal procedan al examen del contenido (y en su caso, aprehensión) de los dispositivos informáticos que se encuentren en dicho domicilio, con el fin de hallar en los mismos cualquier rastro o vestigio que sirva para el descubrimiento del delito y la condena a su responsable. Y sin embargo, la actual habilitación legal en España para proceder al registro e incautación de la información almacenada en los equipos informáticos se deduce de una interpretación *actualizada*[4] por parte de la jurisprudencia de la regulación vigente en la LECrim (Ley de Enjuiciamiento Criminal) del registro de "libros y papeles" (arts. 545 y ss.); de la recogida de los "efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro" (art. 282) y de las normas sobre la

[3] Ley de 25 de diciembre de 2008 de Defensa contra los Peligros del Terrorismo Internacional (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt.* BGBl. I, Nr. 66, S. 3083), que reforma la Ley de 7 de julio de 1997 (*Bundeskriminalamtgesetz*, -BKA-Gesetz-. BGBl. I, S. 1650) El registro online de equipos informáticos se define como "acceso secreto a los equipos informáticos" (*Verdeckter Eingriff in informationstechnische Systeme*, aunque coloquialmente se le denomina *Online Durchsuchung*).

[4] Vid. SSTS de 18 de mayo de 2001 y de 14 de febrero de 2006: "Los preceptos de la L.E.Criminal relativos a la recogida de pruebas materiales de la realización del delito en el lugar de los hechos (art. 326 sobre la inspección ocular; art. 334 sobre el cuerpo del delito, etc), deben ponerse en relación con los arts. 282 y 286.2º de la misma ley y con el Real Decreto 769/1987, de 17 de junio, regulador de las funciones de la Policía Judicial, de cuya combinada aplicación se deduce la interpretación racional y actualizada de la norma en el sentido de que la labor especializada de búsqueda y ocupación de vestigios o pruebas materiales de la perpetración del delito en el lugar de los hechos compete al personal técnico especializado de la Policía Judicial, bajo la superior dirección del Juez Instructor, pero sin necesidad de su intervención personal".

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

"Inspección ocular y del Cuerpo del delito" (arts. 326 y ss.), a pesar de que el Consejo de Europa ya había advertido en 1995[5] sobre la insuficiencia de las leyes de la mayoría de los Estados miembros respecto a la existencia de medidas apropiadas para la búsqueda y aprehensión de las evidencias contenidas en los equipos informáticos, y propugnaba la necesidad de adaptar las medidas de investigación recogidas en la legislación procesal penal a la naturaleza específica de las investigaciones referidas a los sistemas informáticos.

3. 'Remote forensic software': el registro online de equipos informáticos

Los avances tecnológicos actualmente disponibles permiten ir más allá de la aprehensión y el registro *in situ* de equipos informáticos. La "vigilancia online[6]" no sólo permite la interceptación en tiempo real de las comunicaciones electrónicas transmitidas a través de Internet, sino también la adquisición de la información almacenada en soportes informáticos, tanto si éstos se encuentran en los servidores y proveedores de servicios, como si se hallan en los propios equipos de los usuarios, a través de programas espías de tipo *keylogger*[7].

En los EE.UU, la prensa y doctrina se hacían eco en 2001 de la evolución por parte del FBI de los métodos basados en los instrumentos denominados *pen register* y *trap and trace*, a través del desarrollo de un programa informático de vigilancia electrónica capaz de ser instalado de manera remota en el equipo informático del sujeto investigado -"Magic Lantern"-, y registrar todo lo tecleado en el ordenador para conseguir así las contraseñas y los datos almacenados en el mismo[8]. Y en junio de 2007, se daba cuenta del desarrollo de un nuevo programa espía también instalable de forma remota -CIPAV[9] (Computer and Internet Protocol Address Verifier)- que permitiría enviar a través de Internet a otro ordenador (controlado por la autoridad que lleva a cabo la investigación) cierta información recogida del ordenador investigado, como por ejemplo, la dirección IP o MAC del equipo, puertos TCP y UDP, los programas ejecutados, el tipo del sistema operativo utilizado, así como su versión y su número de serie, el navegador, las contraseñas almacenadas en el equipo, las direcciones IP con las que conecte el equipo investigado o las últimas direcciones URL visitadas, pero sin llegar a acceder ni grabar el contenido de dichas comunicaciones, razón por la cual la Novena Corte de Apelación de San Francisco ha comparado dicha investigación de equipos informáticos con los *pen register*[10].

[5] Vid. Recomendación R (95) 13, del Comité de ministros del Consejo de Europa, de 11 de septiembre de 1995, relativa a los problemas de la legislación procesal penal conectados a las tecnologías de la información.

[6] La doctrina norteamericana utiliza los términos "electronic surveillance", "Internet surveillance" y "online surveillance". Vid. BELLIA, P.: "The future of internet surveillance", *The George Washington Law Review*, August, 2004, 72, p. 1375 y ss.; FREIWALD, S.: "Online Surveillance: Remembering the Lessons of the Wiretap Act", *Alabama Law Review*, Fall, 2004, 56, p. 9 y ss.

[7] Procedente de la abreviatura *keystroke logger* ("registrador de pulsación de tecla"): un programa que permite registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero del propio ordenador intervenido y/o enviarlas a través de Internet.

[8] Vid. http://www.news.com/FBI-snoop-tool-old-hat-for-hackers/2100-1001_3-276145.html; http://www.merit.edu/mail.archives/netsec/2001-05/msg00002.html. En la doctrina, vid. MARTIN, R. S.: "Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome", *American Criminal Law Review*, Vol. 40, 2003; WOO, C. / SO, M.: "The case for Magic Lantern: September 11 Highlights. The need for increased surveillance", *Harvard Journal of Law & Technology*, Vol. 15, 2002.

[9] Vid. el affidávit solicitado por el FBI para proceder a la instalación del programa CIPAV (http://politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf) y la autorización judicial (http://politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf), así como las noticias publicadas en Internet: http://news.com.com/8301-10784_3-9746451-7.html, http://www.wired.com/politics/law/news/2007/07/fbi_spyware.

[10] Vid. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/07/07/BAGMNQSJDA1.DTL&tsp=1. Desde los casos *Smith v. Maryland* [442 U.S. 735 (1979)] y United States v. New York Tel. Co. [434 U.S. 159, 161 n.1 (1977)], el Tribunal Supremo norteamericano ha afirmado que no existe una expectativa razonable de privacidad (*reasonable expectation of privacy*) afectada por el uso de un *pen register*.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

En Alemania, parte de la doctrina había defendido la admisibilidad de los "registros online" sobre la base legal de las entradas y registros tradicionales regulados en los §§ 102 y ss. del Código Procesal Penal alemán (StPO), en relación con la cláusula general de investigación del § 161[11], pero el Tribunal Supremo alemán, en su Auto de 31 de enero de 2007[12], declaró que la infiltración secreta que constituye el registro online carecía de fundamento legal y por tanto no resultaba admisible como medida procesal de investigación. Fue el Estado de Renania del Norte-Westfalia el que por primera vez legisló sobre el acceso secreto a los equipos informáticos como medida policial de investigación, y si bien es cierto que la Ley de Renania del Norte fue declarada inconstitucional mediante la Sentencia del Tribunal Constitucional Federal de de 27 de febrero de 2008[13], dicha sentencia resulta especialmente destacable por dos motivos.

En primer lugar, porque en dicha sentencia se enuncia un nuevo Derecho Fundamental, incardinado dentro del Derecho a la Autodeterminación informativa: *el Derecho Fundamental a la garantía de la confidencialidad e integridad de los equipos informáticos (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)*. Ello, tras reconocer que las garantías legales y constitucionales derivadas de los Derechos al secreto de las comunicaciones e inviolabilidad del domicilio, así como las acuñaciones que del Derecho a la Personalidad se habían hecho a través de la jurisprudencia constitucional, no habían tenido suficientemente en cuenta la necesidad de protección de la intimidad frente al desarrollo de las técnicas informáticas, por lo que su cobertura resultaba insuficiente para dicha protección.

Según el Tribunal germano, el Derecho fundamental a la inviolabilidad del domicilio resulta insuficiente porque los equipos informáticos no pueden tener la consideración de "domicilio" a efectos constitucionales[14], lo cual limita la protección constitucional de dicho Derecho Fundamental a aquellos supuestos en los que, para llevar a cabo el registro online del equipo informático, previamente se tenga que entrar físicamente en el domicilio para la instalación del software o hardware necesario. Tampoco resultarían aplicables las garantías que acompañan a la medida conocida como *Großes Lauschangriff*[15], que permite a la policía tener conocimiento de lo que sucede en el interior del domicilio sin necesidad de acceder al mismo, mediante el empleo de instrumentos acústicos, ópticos o de medición de las radiaciones electromagnéticas, porque no se protegerían aquellos sistemas informáticos que no se encuentren físicamente en el domicilio del afectado, lo cual resulta cada vez más habitual si tenemos en cuenta la movilidad de los actuales dispositivos (ordenadores portátiles, PDA's, teléfonos móviles).

[11] Vid. BÄR, W.: "Polizeilicher Zugriff auf kriminelle Mailboxen", CR 1995, p. 489; ZÖLLER, M. A.: "Verdachtslose Recherchen und Ermittlungen im Internet", GA 2000, p. 563; HOFMANN, M.: "Die Online-Durchsuchung - staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ 2005, Heft 3, p. 121; KEMPER: "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP 2007, Heft 4, p. 107.

[12] BGH, Beschluß vom 31. 1. 2007 - StB 18/06.

[13] BverfG, 1 BvR 370/07 de 27.2.2008.

[14] Cfr., SCHLEGEL, S.: "Warum die Festplatte keine Wohnung ist - Art. 13 GG und die '"Online-Durchsuchung"", *LSK* 2007-2, ref. 500336.

[15] Vid. KUTSCHA: "Der Lauschangriff im Polizeirecht der Länder", NJW 1994, Heft 2, p. 85; BENFER: "Großer Lauschangriff" - einmal ganz anders gesehen, NVwZ 1999, Heft 3, p. 237; PFEIFFER: "Akustische Überwachung von Wohnungen", Karlsruher Kommentar zur StPO, 5. Auflage, 2003, Rn 32c; BRAUN: "Der so genannte " Lauschangriff " im präventivpolizeilichen Bereich - Die Neuregelung in Art. 13 IV-VI GG", NVwZ 2000, Heft 4, p. 375; GUSY: "Lauschangriff und Grundgesetz", JuS 2004, Heft 6, p. 457; JEKEWITZ: "Das Urteil des Bundesverfassungsgerichts zu den Grundlagen der akustischen Wohnraumüberwachung in Art. 13 Abs. 3 GG", en VV.AA.: Geldwäschebekämpfung und Gewinnabschöpfung, 1. Auflage 2006, Rn 8-12.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Y el Derecho fundamental al secreto de las comunicaciones tampoco protege la integridad de los equipos informáticos de los ciudadanos frente a infiltraciones secretas y remotas, pues con la medida consistente en el registro *online* de dichos equipos no se pretende exactamente "intervenir" o "interceptar" una comunicación o tomar conocimiento de su contenido, existencia, o circunstancias en las que tuvo lugar, sino "acceder", a través de las vías de comunicación existentes, al interior de un equipo informático con el objetivo de inspeccionar y/o remitir el contenido del mismo.

Ahora bien, esta idea no es nueva. La insuficiencia de la protección constitucional y legal de la intimidad, la inviolabilidad del domicilio, o el secreto de las comunicaciones para hacer frente a los retos que la revolución tecnológica suscita, y que se plantean en la persecución penal en el entorno digital, ya fue puesta de manifiesto por GONZÁLEZ-CUÉLLAR SERRANO en el año 2006 en su magnífico trabajo "Garantías Constitucionales en la persecución penal en el entorno digital ", quien aludía específicamente a los peligros derivados de una posible infiltración en los dispositivos y equipos informáticos poseídos por las personas y proponía incluir bajo el manto protector del Derecho Fundamental a la libertad informática del art. 18.4 CE, el denominado "*Derecho a la no intromisión en el entorno digital del individuo*" para dotar a dicho entorno digital de una cobertura integral que integrara todas aquellas garantías proporcionadas por otras normas constitucionales de protección de los derechos fundamentales (v. gr., la inviolabilidad del domicilio y el secreto a las comunicaciones) con las que podría solaparse en parte.

En segundo lugar, la citada sentencia del Tribunal Constitucional Federal germano resulta trascendental para la evolución de la regulación de medidas procesales de investigación basadas en el uso de la Informática porque, a pesar de la declaración de inconstitucionalidad de la Ley de Renania del Norte, estableció los requisitos que debería cumplir aquella ley que regulara tales registros online para ser compatible con las garantías constitucionales. Requisitos que pueden quedar resumidos en tres: a) la existencia de una autorización judicial previa para proceder a la infiltración secreta y remota en los diversos equipos electrónicos e informáticos; b) la existencia de datos fácticos de un concreto peligro para un bien jurídico "especialmente destacable" (*überragend wichtiges Rechtsgut*), entendiendo el Tribunal Constitucional por especialmente destacables "el cuerpo, la vida y la libertad de la persona o semejantes bienes de la Comunidad, cuya amenaza afecte a los Fundamentos o a la propia existencia del Estado o a los fundamentos o existencia de las personas"; y c) las disposiciones necesarias para proteger el núcleo esencial del desarrollo de la vida privada (*Kernbereich privater Lebensgestaltung*).

El gobierno federal alemán ha respetado dichos requisitos a la hora de reformar la BKA-Gesetz y regular importantes y avanzadas medidas tecnológicas de investigación, entre las que se encuentra el registro online de equipos informáticos, mediante la citada Ley de 25 de diciembre de 2008 de "Defensa contra los Peligros del Terrorismo Internacional".

[16] GONZÁLEZ-CUÉLLAR SERRANO, N.: "Garantías Constitucionales en la persecución penal en el entorno digital", en Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García, ed. Colex, Madrid, 2006, p. 890.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

El título de dicha Ley no es baladí, pues aún cuando el Tribunal Constitucional no lo declarase explícitamente en su sentencia, a lo largo de la misma menciona más de una docena de veces el término "terrorismo", y más concretamente habla de "terrorismo internacional", "terrorismo extremista", y "terrorismo islámico", y reconoce que el aumento del terrorismo internacional ha generado una nueva amenaza que obliga al Estado a establecer limitaciones de los Derechos Fundamentales en interés de conseguir una defensa efectiva contra el terror, de modo que un Estado de Derecho tiene la obligación de desarrollar y ampliar los instrumentos legales tradicionales, y en especial, tiene que ampliar las capacidades operativas informáticas de las fuerzas de seguridad. De ahí que el § 4a de la citada Ley de 25 de diciembre de 2008 establezca que dichas medidas excepcionales de investigación se utilizarán únicamente en los casos relacionados con el terrorismo internacional y con los delitos mencionados en el art. 129a del Código Penal alemán (organizaciones criminales terroristas).

4. Conclusión: La necesaria reforma procesal en España

La posibilidad de acceder de forma remota a los datos almacenados en un equipo informático representa un avance tecnológico muy eficaz a la hora de ser empleado como medida de investigación en la lucha contra el terrorismo, pues proporciona a las autoridades la posibilidad de acceder a una valiosa fuente de prueba sin necesidad de tener que conseguir la localización física y el registro *in situ* de dicho equipo para obtener la información almacenada en el mismo, con el consiguiente riesgo de que, para entonces, dichas evidencias (caracterizadas por su perentoriedad y su alterabilidad) hayan sido destruidas.

La legislación procesal española, sin embargo, se encuentra obsoleta y desfasada con respecto a los desafíos que plantean las nuevas tecnologías, y ha tenido que ser colmada jurisprudencialmente, como demuestra la vasta doctrina del Tribunal Supremo y el Tribunal Constitucional con respecto a la intervención de las telecomunicaciones, y motivo por el cual el TEDH ha condenado en dos ocasiones a España[17]. La inexistencia de una normativa expresa que regule la posibilidad de utilizar los nuevos avances tecnológicos, en la consecución de los legítimos fines de investigación criminal, supone acrecentar las desventajas con las que se encuentran las fuerzas y cuerpos de seguridad a la hora de proceder a la indagación y descubrimiento de los instrumentos y pruebas de los delitos, así como para la identificación de sus responsables, sobre todo en lo relacionado con la criminalidad informática. Pero no es posible justificar el empleo de cualesquiera métodos de investigación, sin una mínima base legal que regule sus garantías, requisitos y límites, bajo la excusa de poder contrarrestar así los avances con los que cada día cuentan los criminales para cometer sus delitos[18].

[17] SSTEDH de 30 de abril de 1998 (Valenzuela Contreras c. España) y de 18 de febrero de 2003 (Prado Bugallo c. España), aunque dicha doctrina a favor de la labor jurisprudencial integradora de las lagunas legales en materia de intervención de las comunicaciones ha sido finalmente respaldada por el TEDH en su Auto de Inadmisión de 25 de septiembre de 2006 (caso Abdulkadir Coban c. España).

[18] No compartimos el argumento de VELASCO NÚÑEZ ("Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos)", en VV.AA.: Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 107) de que los instrumentos de trabajo de la policía deben ponerse a la altura de los tiempos y entenderse que el ejercicio de las facultades legales que les procura el art. 22.2 LOPDP y el 12.3 LSSICE son autónomamente compatibles con la supervisión judicial de los Derechos Fundamentales del investigado, y la corrección a los hipotéticos excesos, fraudes o posibles abusos que pudieran darse, encontrarla más bien en la responsabilidad penal o disciplinaria del concreto investigador, que en la forzada nulidad probatoria (que más que corregir futuras actuaciones policiales, aboca en impunidades intolerables y en "castigos" a la inocente Sociedad que debe soportarlas).

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

cybex
The Digital Forensic Company

La respuesta del Estado de Derecho frente a la utilización de la informática para la preparación y realización de las más diversas modalidades delictivas debe ser la reforma del ordenamiento jurídico para valerse de las modernas técnicas de investigación que la Informática proporciona e implementar las medidas policiales y procesales para la prevención e investigación de los delitos, sobre todo aquellos que se basan en la utilización de la Informática, porque debido a la enorme injerencia y especial gravosidad que el registro de equipos informáticos representa para los Derechos Fundamentales a la intimidad, secreto de las comunicaciones, inviolabilidad del domicilio, secreto profesional, etc., no consideramos posible una aplicación analógica, ni siquiera con carácter provisional, de la regulación establecida respecto de otras medidas de investigación que puedan guardar cierta relación con dicho registro[19].

No obstante lo anterior, y debido a la desidia de nuestro legislador en acometer tales reformas, la postura mantenida por el Tribunal Supremo ha sido legitimar determinadas prácticas policiales, sobre la base de dicha aplicación analógica y bajo la cobertura de la supuesta proporcionalidad de las mismas, de un modo tal que no se satisfacen las mínimas exigencias de legalidad y claridad establecidas por el TEDH, que ha declarado indispensable que *las normas sean claras y detalladas, tanto más cuanto que los procedimientos técnicos utilizables se perfeccionan continuamente* , lo cual es perfectamente predicable del entorno digital.

Así, por ejemplo, en su momento llegó a admitir la facultad policial de proceder a la indagación de la memoria de los teléfonos móviles sin necesidad de autorización judicial previa, dentro de sus legítimas facultades de registro superficial de la persona detenida y de ocupación de las pertenencias que ésta porta consigo, al equiparar la agenda electrónica del aparato de telefonía con cualquier otra agenda en la que el titular puede guardar números de teléfonos y anotaciones sobre las realizadas y llamadas, y negarle la consideración de teléfono en funciones de transmisión de pensamientos dentro de una relación privada entre dos personas[21]. Si admitimos dicha postura, ¿qué diferencia habría entonces entre examinar la memoria de un teléfono móvil con respecto a la memoria de una PDA, un reproductor mp4, una memoria USB, o incluso, el disco duro de un ordenador portátil que el sujeto lleve consigo? En los EE.UU., la doctrina *Robinson*[22] permite a los agentes de policía llevar a cabo un registro completo del individuo tras un arresto legal, amparado en la necesidad general de preservar las evidencias del delito y evitar posibles daños al agente que efectúa el arresto. Pero el hecho de que la policía pueda examinar el contenido de pertenencias tales como carteras, agendas o maletines sin necesidad de autorización judicial no debe ampliarse al registro de sus pertenencias electrónicas (agendas electrónicas, diskettes, etc), dada la desproporcionalidad al respecto[23].

[19] Vid. FERNÁNDEZ RODRÍGUEZ, J. J.: *Secreto e intervención de las comunicaciones en Internet*, ed. Thomson-Civitas, Madrid, 2004, p. 153, y GONZÁLEZ LÓPEZ, J. J.: *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal*, ed. La Ley, Madrid, 2007, p. 189.

[20] Vid. SSTEDH *Kruslin y Huvig c. Francia de* 24 de abril de 1990: "*la ley debe ser lo suficientemente clara para señalar a todos las circunstancias y condiciones en que autoriza a los poderes públicos a recurrir a una injerencia así, secreta y posiblemente peligrosa, en el derecho al respeto de la vida privada y de la correspondencia*".

[21] Vid. SSTS de 27 de junio de 2002, 25 de julio de 2003 y 25 de septiembre de 2003. A favor de dicha postura, VELASCO NÚÑEZ ("Eliminación de contenidos ilícitos...", op. cit., p. 114). En contra, vid. GONZÁLEZ-CUÉLLAR SERRANO ("Garantías constitucionales...", op. Cit., p. 915), para quien tampoco cabrían los registros de dichos dispositivos, al amparo de los controles de identidad en lugares o establecimientos públicos previstas por el art. 19.2 de la L.O. 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.

[22] Vid. United States v. Robinson, 414 U.S. 218, 235 (1973).

[23] KERR, O.: "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", July 2002, p. 22: "*Ante la increíble capacidad de almacenamiento de los dispositivos electrónicos, la doctrina Robinson puede no ser siempre aplicable en los casos de los registros electrónicos. Y en caso de duda, los agentes deberían considerar la necesidad de conseguir una autorización judicial antes de examinar el contenido de los aparatos electrónicos de almacenamiento que pueden contener enormes cantidades de información*".

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Dicha línea jurisprudencial fue afortunadamente abandonada en su STS de 8 de abril de 2008, tras hacerse eco de la STC 230/2007, pero existen otros casos en los que nuestro Tribunal Supremo ha mantenido una interpretación rigorista y restrictiva de las garantías constitucionales y legales con respecto al uso de las nuevas tecnologías en la investigación criminal. En la STS de 20 de mayo de 2008, secundada por la STS de 18 de noviembre de 2008, el Tribunal Supremo ha declarado que la captación por parte de la policía, y sin autorización judicial previa, del número IMSI correspondiente a un terminal de telefonía móvil no conculca el Derecho Fundamental al secreto de las comunicaciones del art. 18.3 CE porque dicho número no debe considerarse dentro de los *datos de tráfico* generados con motivo de una comunicación telefónica, sino como un *dato de carácter personal* relacionado con el art. 18.4 CE, de modo que el régimen jurídico que regularía su obtención sería el referido a la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad (L.O. 15/1999, de 13 de diciembre) y no el referido a la petición de su cesión por parte de las operadoras (Ley 25/2007, 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones). Ahora bien, legitimar la aprehensión policial, sin una orden judicial previa, de determinada información que se considera como "datos personales", resulta cuestionable a la par que arriesgado.

Cuestionable porque el número IMSI constituye un dato identificativo del origen de una determinada comunicación telefónica, y por lo tanto, estaría amparado por el derecho al secreto de las comunicaciones, porque sin el mismo no podría tener lugar la comunicación a través de la telefonía móvil[24]. Y en apoyo de esta interpretación vemos que el gobierno de los EE.UU ha reconocido que dicho número IMSI constituye un dato necesario para que la comunicación tenga lugar, y además, con los instrumentos utilizados para la obtención de dicho número (*digital analyzers* o *cell site simulators*, también denominados "triggerfish"), es posible conseguir el número del teléfono móvil desde el cual se inicia la comunicación, el número marcado, la fecha, hora y duración de la llamada, la celda de localización desde donde el teléfono móvil comenzó la conversación, e incluso, los contenidos de la misma, si bien tales instrumentos pueden ser configurados para omitir dicha información[25].

Y arriesgado porque abre la puerta a futuras aprehensiones de datos electrónicos por parte de la policía sin orden judicial, con la excusa de que se trate de *datos necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales* (art. 22.2 de la L.O. 15/1999), pues el Tribunal Supremo ha admitido que "la capacidad de recogida de datos que la LO 15/1999, 13 de diciembre, otorga a las Fuerzas y Cuerpos de Seguridad del Estado, no puede, desde luego, servir de excusa para la creación de un régimen incontrolado de excepcionalidad a su favor. Pero tampoco cabe desconocer que la recogida de ese dato en el marco de una investigación criminal -nunca con carácter puramente exploratorio-, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional".

[24] Vid. RODRÍGUEZ LÁINZ ("Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", Diario La Ley, 2009, nº 7086, pp. 1-11) a favor de la consideración del número IMSI como un dato de tráfico amparable en la protección del art. 18.3 CE. A favor de dicha captación sin orden judicial, vid. INZA, J.: "Obtención del IMSI sin autorización judicial", en http://inza.wordpress.com/2008/10/09/obtencion-del-imsi-sin-autorizacion-judicial/.

[25] Vid. El documento *Electronic Surveillance Manual*, elaborado por la Unidad de vigilancia electrónica de la División Criminal, p. 41: "If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/ triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected). Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function (...)".

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Ante dicha postura, sólo es cuestión de tiempo que en España se solicite, o se lleve a cabo, la instalación remota en el equipo informático del sospechoso del software necesario para recabar aquella información que la policía estime necesaria para la averiguación del delito investigado[26], y no puede pasarse por alto que ya ha habido algún pronunciamiento judicial relativo al uso de estos programas entre particulares, y que acabó en sentencia condenatoria por delito de revelación de secretos[27].

Por ello, consideramos necesaria una profunda reforma de la LECrim que incluya como medida de investigación, de forma expresa y detallada, el registro de equipos informáticos -el registro *online* no sería más que una modalidad en cuanto al modo de proceder al registro de los equipos-, y en general, regule expresamente la posibilidad de utilizar los nuevos avances tecnológicos en los ámbitos policial y judicial, de un modo que constituya un verdadero desarrollo del Derecho Fundamental a la libertad informática recogido en el art. 18.4 CE, en su vertiente de "Derecho a la no intromisión en el entorno digital del individuo" propuesta por -CUÉLLAR SERRANO.

[26] S A favor de la utilización de los programas *keylogger* y *e-blaster* en la investigación penal, vid. URBANO DE CASTRILLO, E.: "La investigación tecnológica del delito", en VV.AA.: *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 65.
[27] SAP Madrid, Secc. 17°, de 25 de mayo de 2005.

Editores de la Sección: Esther George y Pedro Verdelho

El objetivo de la sección jurídica del ENAC es describir y tratar los temas más relevantes, tanto a nivel internacional como nacional, especialmente en Europa, pero también en América, Asia o África, en referencia al desarrollo de la cibercriminalidad y las nuevas leyes adoptadas. Todas las contribuciones de los lectores son bienvenidas, mediante comentarios o enviando artículos para su publicación. Si Usted tiene un punto de vista sobre alguno de estos temas que quiera compartir, no dude en ponerse en contacto

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

RAMÓN MIRALLES
Coordinador de Auditoria i Seguridad de la Información · Agencia Catalana de Protección de Datos

PRIVACY BY DESIGN: LA PRIVACIDAD EN EL DISEÑO

La prevención en materia de protección de datos de carácter personal resulta especialmente relevante y útil cuando los datos objeto de tratamiento son sensibles, o las necesidades de explotación de la información implican compartir o intercambiar datos entre sistemas de información.

Por ello, todo aquello que permita evitar que se produzca un incidente con los datos personales va a ser mucho más eficiente, tanto para los afectados como para los responsables del tratamiento. La prevención es lo que realmente puede garantizar un adecuado clima de confianza y seguridad, y una gestión responsable de la información de carácter personal.

En la Directiva 95/46/CE hay algunos preceptos donde la prevención aparece claramente identificada, destacaremos especialmente el considerando 46:

> *"Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;"*

A los efectos que nos interesan aquí se alude en este considerando a que ya durante el diseño del tratamiento se tenga en cuenta todo aquello, tanto de índole técnica como organizativa, que permita evitar incidentes que afecten a la información de carácter personal.

En la práctica nuestras normas de protección de datos suelen llevar a los responsables de tratamientos a tener una actitud ante la privacidad que fundamentalmente gira entorno a la pregunta de:

"¿Como afecta la normativa en materia de protección de datos de carácter personal a mi actividad?"

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

En lugar de recurrir a un modelo donde la pregunta debería ser:

"¿Cómo al tratar datos de carácter personal puedo estar impactando o incidiendo en la privacidad de las personas?"

Se pueden dar dos tipos de actitud en relación a la ejecución de proyectos en los que se vean involucrados datos de carácter personal:

a) Aquellas actitudes en las cuales los aspectos de seguridad de la información y privacidad (protección de datos) se tienen en cuenta al final del proyecto, es decir, se diseña la solución teniendo en cuenta exclusivamente los requerimientos de negocio (temporales y/o funcionales), por tanto se busca solo un cumplimiento formal de la norma.

b) Aquellas otras situaciones, las menos, en que durante la fase de diseño, por tanto desde el inicio, se tienen en cuenta también los requisitos de seguridad de la información y de privacidad

Las consecuencias de una u otra actitud son bien diferentes:

a) Para el primero de los planteamientos la seguridad y la protección de datos de carácter personal son un obstáculo o una barrera que frena el normal desarrollo del proyecto y que, por tanto, afecta a los objetivos perseguidos, tanto a los funcionales como a los temporales, la realización del proyecto entra en zona de riesgo por culpa ya sea de la seguridad o de la protección de datos

b) Al tenerse en cuenta desde el inicio de un proyecto la seguridad y la protección de datos, en la misma fase de diseño, éstas no se visualizan como obstáculos, sino que más bien al contrario, añaden elementos de confianza en el nuevo sistema, y en algunos casos mejoran sustancialmente la calidad y aceptación del mismo

Para ir hacia las situaciones y consecuencias descritas en el caso "b" debemos abordar la privacidad en el diseño de los proyectos, servicios y aplicaciones, es lo que, utilizando el término anglosajón se conoce como *privacy by design* (privacidad en el diseño).

Vendría a ser la idea utilizada en el mundo del desarrollo de software o de la implantación de soluciones técnicas conocida como "seguridad en el diseño", que no es otra cosa que marcarse como objetivo la seguridad desde la fase inicial del diseño técnico.

El "privacy by design" es un modelo en construcción, de hecho estará presente en la próxima "Conferencia Internacional de Autoridades de Protección de Datos y Privacidad", que se celebrará en Madrid el próximo mes de noviembre, des de la Agencia Catalana de Protección de Datos trabajamos en la identificación y análisis de propuestas innovadoras que faciliten la prevención, en esa línea estamos construyendo un modelo teórico de

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

prevención basado en promover que las cuestiones relacionadas con el tratamiento de datos de carácter personal se incorporen en las iniciativas y proyectos en la misma fase en que se diseñan las funcionalidades y contenidos, de manera que los gestores de los proyectes puedan definir soluciones que permitan una eficaz y ágil gestión de la información y a la vez los principios del derecho fundamental a la protección de datos de carácter personal sean respetados, es decir, que se dé correcta respuesta a los requisitos de las normas.

Como primeros resultados de los trabajos realizados en este ámbito preventivo se ha definido un modelo inicial de privacidad en el diseño, que va más allá del cumplimiento del marco jurídico vigente, y que aglutina propuestas y soluciones aportadas por el mercado y por los investigadores a nivel internacional, en resumen la propuesta de la APDCAT puede resultar una herramienta clave para prevenir y tratar las cuestiones derivadas de la privacidad y la protección de datos personales, incorporando elementos de seguridad y privacidad en el diseño de las soluciones de gestión de la información personal.

Una de les tareas que la APDCAT ha realizado es dar estructura y contenidos a ese modelo, de manera que pueda ser aplicado con facilidad por las organizaciones que tratan datos personales, tanto del sector público como privado, de una manera directa y con una visión absolutamente pragmática.

El que prevé la propuesta de la Agencia es explotar el concepto de *privacy by design*, que implica incluir soluciones de seguridad y privacidad en el momento de diseñar los procesos involucradas en los tratamientos de datos de carácter personal, así como en el momento de definir la organización que ha de controlar y gestionar la aplicación de los criterios de privacidad y/o seguridad, o a la hora de seleccionar la tecnología utilizada para tratar la información, ya que las tres cuestiones (procesos, organización y tecnología) tienen una incidencia directa en la gestión de la información de carácter personal.

Respecto de los **procesos** algunas de las soluciones que permiten incorporar una privacidad en el diseño son:

·La evaluación del impacto sobre la privacidad (*Privacy Impact Assessment – PIA*), es decir, un sistema metódico para determinar los efectos de los programas de actuación y la prestación de servicios públicos sobre la privacidad de las personas, de manera que la PIA es una metodología útil para garantizar, al inicio de todo nuevo programa o servicio, que se construirá respetando los principios de privacidad, a la vez que se garantiza a la opinión pública que su privacidad está salvaguardada.

Aunque se plantea como una evaluación a priori, también, se pueden someter a este proceso de evaluación sistemas o servicios que ya están operativos, la dificultad se centrará entonces en si será posible, y con qué costes, adaptar los sistemas preexistentes al resultado de la evaluación, de aquí la importancia de realizar, como regla general, este proceso de reflexión como requisito previo al diseño funcional de las soluciones.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

·Mecanismos de mejora de la información, referida a los tratamientos, que se proporciona a les personas afectadas (*Fair Processing Notifications – FPN y Multilayered Privacy Notice*), es decir, diseñar políticas informativas comprensibles y coherentes sobre los tratamientos de datos personales, en definitiva, máxima transparencia.

·Gestión de las opciones y preferencias de privacidad de los usuarios (*Customer Preference and Choice – CPC*), es decir, disponer de mecanismos efectivos y ágiles para conocer y gestionar qué opciones relacionadas con el tratamiento de sus datos personales ha seleccionado una persona concreta.

·La seguridad diseñada entorno a los datos y los usuarios que los tratan (*Information-Centric Security*). No es otra cosa que una orientación técnica de como diseñar la arquitectura de seguridad de los sistemas, que se puede plantear de fuera a dentro, o de dentro hacia afuera, en este caso se plantea que lo importante es proteger la información, por tanto la arquitectura de seguridad da respuesta en primer lugar a los requerimientos técnicos y legales de protección de los datos personales.

En cuanto a soluciones relacionadas con el diseño de la organización tenemos figuras organizativas como:

·Responsable de protección de datos o "*Data protection Officer*" – DPO, según la nomenclatura anglosajona, y que se puede asimilar a la figura del SPOC (single point of contact) de ITIL (Biblioteca de Infraestructura de Tecnologías de la Información, es un estándar de facto para la gestión de servicios informáticos); con el DPO todas las cuestiones relacionadas con los tratamientos de datos de carácter personal, y en especial aquello relacionado con la conformidad normativa, pasan por una persona especializada en la materia, que aglutina conocimientos y características de perfiles profesionales jurídicos, tecnológicos y de gestión. Esta figura no ha sido regulada en la legislación española.

·Responsable de seguridad: encargado de coordinar la implantación de las medidas de seguridad y de controlar su eficacia. En la legislación española de protección de datos es una figura perfectamente definida en cuanto a sus funciones en relación a las medidas de seguridad de los tratamientos de datos de carácter personal.

·La existencia de departamentos de auditoria que facilita una revisión continuada de los procesos para comprobar que se realizan según lo previsto y que, por tanto, se dan los resultados esperados; la actividad de auditoria permite detectar deficiencias en los sistemas y proveer los mecanismos correctivos.

·Los comités de seguridad permiten tomar decisiones relacionadas con la seguridad y con la participación de las áreas clave de las organizaciones, de manera que no solo las decisiones están suficientemente consensuadas, sino que además toda la organización se involucra en las decisiones tomadas y las hacen suyas; los comités requieren de la participación y soporte de los niveles directivos de las entidades a fin de dar la mayor fuerza posible a sus decisiones.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Y por último también en la implantación de las soluciones tecnológicas puede jugar un importante papel tener en cuenta la privacidad, seleccionando aquellas soluciones que aporten prestaciones para tratar la información teniendo en cuenta los requisitos derivados del uso de información de carácter personal, así tenemos:

·Las tecnologías orientadas a reforzar la privacidad (*Privacy Enhancement Technologies - PET*), un concepto que aglutina aquellas soluciones de mercado que entre sus prestaciones incluyen elementos especialmente sensibles con la privacidad (anonimato, disociación de información, auditoria, cifrado, etc).

·Las tecnologías y soluciones que tienen activadas por defecto las opciones de privacidad más restrictivas (*Privacy by default*), en contraposición a aquellas soluciones que plantean el acceso a toda la información y se deben ir limitando los niveles de difusión de la información de carácter personal.

·Metadatos en los intercambios de información de carácter personal o lenguajes específicos para autorizaciones relacionadas con el uso de datos personales y el acceso a los datos (como por ejemplo, *Enterprise Privacy Authorization Language – EPAL de IBM* o el *eXtensible Access Control Markup Language – XACML* de Sun Microsystems), en definitiva se trata de diseñar modelos de metadatos para el intercambio de información de carácter personal (MDP), que garantice el cumplimento de la normativa de protección de datos y facilite la gestión de la información compartida o intercambiada.

·Tecnologías para detectar y prevenir transmisiones no autorizadas de información fuera de las organizaciones (*Data Loss Prevention - DLP*), que permiten controlar los flujos de información y los mecanismos de transporte y almacenamiento de la información, incluso a nivel físico, de manera que se minimiza el riesgo de pérdida o fuga de información fuera de los ambientes de control.

Todo este conjunto de soluciones o propuestas, y otras que sin duda se irán incorporando, englobadas bajo el concepto de *privacy by design* pueden ser herramientas claves para abordar de una manera eficiente y eficaz la prevención en materia de protección de datos de carácter personal, obviamente no todas las propuestas son adecuadas para todas las organizaciones, deben adoptarse aquellas que resulten útiles, en función de las necesidades y particularidades de cada organización y de los tratamientos que son de su responsabilidad.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Editora de la Sección: Elena Domínguez Peco

Esta sección presentará las novedades que presentan la legislación nacional e internacional en protección de datos, siempre en relación con la lucha contra el cibercrimen. Si desea colaborar en la elaboración de la sección, aportar contenido o proporcionar su opinión, por favor póngase en contacto con la editora.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

JOSÉ DUART
Experto en ingeniería inversa y análisis forense
NIVEL DE DIFICULTAD TÉCNICA IIIII*

TÉCNICAS ANTI FORENSES EN NTFS

Desde el momento en que algunas personas comenzaron a trabajar con grandes cantidades de información a las que se accedía desde un único ordenador, empezaron también a imaginar formas de mantener oculta dicha información para los demás usuarios. Probablemente, dichas ideas constituyeron el germen de los métodos, las herramientas y las técnicas que conocemos hoy en día como técnicas anti forenses. Si se prefiere una definición más formal, hablamos de técnicas anti forenses cuando nos referimos a los métodos o las herramientas diseñados para transformar una pieza de información (una prueba) de manera que permanezca oculta para las herramientas y los procesos habitualmente utilizados en las investigaciones con informática forense.

La popularidad de los métodos y las herramientas anti forenses ha tenido altibajos a lo largo de los años, en función de la comercialización de nuevos sistemas de archivos, sistemas operativos o dispositivos de almacenamiento. Este artículo abordará un método sencillo de evasión forense en el que se emplea uno de los sistemas de archivos más utilizados, el sistema de archivos NT File System (NTFS).

Nociones básicas de NTFS

Para todos aquellos que no conozcan el concepto de sistema de archivos o, concretamente, NTFS, a continuación se ofrecen unas nociones básicas sobre su funcionamiento y sobre algunas estructuras que participan en dicho proceso.

NTFS es un sistema de archivos con registro de transacciones que almacena todos los datos por medio de una estructura de tabla llamada MFT o Master File Table (tabla maestra de archivos). Esta tabla es como una base de datos que contiene la información necesaria para acceder a todos los archivos. Hablamos únicamente de archivos porque la MFT no hace diferencia entre archivos, carpetas y archivos NTFS especiales, como la propia MFT (la MFT se refiere a sí misma como el archivo $MFT). Esto nos lleva a hablar del uso de archivos especiales: en NTFS, todos los datos adicionales necesarios para que funcione el sistema de archivos se almacenan en archivos especiales denominados "archivos de metadatos NTFS". Estos archivos especiales se almacenan siempre en las mismas posiciones de la MFT:

* Nivel de dificultad técnica: Esta marca expone el nivel conocimientos técnicos que se necesitan para el correcto entendimiento del artículo. En este caso es ALTO.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

MFT Table Position	File Name
0	$MFT
1	$MftMirr
2	$LogFile
3	$Volume
4	$AttrDef
5	(Root directory)
6	$Bitmap
7	$Boot
8	$BadClus
9	$Secure
10	$Upcase
11	$Extend
12..15	(Reserved for future use)

Procedamos a describir brevemente cada archivo:

·**$MFT**: la propia tabla.
·**$MftMirr:** una copia de las cuatro primeras posiciones de la tabla MFT para poder recuperar parte de la original en caso de corrupción.
·**$LogFile:** archivo que mantiene un registro de las operaciones internas del sistema de archivos. NTFS se basa en transacciones, por lo que es necesario poder validar operaciones y volver al estado anterior a las mismas, como en las bases de datos.
·**$Volume**: contiene metadatos acerca del volumen, como el nombre o los atributos, si debe verificarse en el siguiente inicio, etc.
·**$AttrDef**: este archivo indica todos los atributos de NTFS permitidos en el volumen. Lo veremos con más detalle posteriormente.
·**(Directorio raíz)**: el directorio raíz; por ejemplo, C:\.
·**$Bitmap**: este archivo mantiene un registro de las entradas de la MFT que se están utilizando.
·**$Boot**: sector de arranque Volume Boot Record del volumen, donde se encuentra el control de transferencia de la BIOS para que arranque el sistema operativo.
·**$BadClus**: es como el archivo $Bitmap pero se utiliza para marcar clústeres dañados que no deben utilizarse.
·**$Secure**: se trata de una base de datos de descriptores de seguridad (ID, ID de grupo, etc.) que utilizan todos los archivos y las carpetas para controlar el acceso de los usuarios.
·**$Upcase**: se trata de un simple archivo que contiene un mapa con caracteres Unicode y su representación en mayúsculas.
·**$Extend**: directorio que contiene archivos de metadatos adicionales o ampliados.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Acabamos de presentar una buena colección de archivos de metadatos con los que esperamos que se hagan una idea de la organización de los sistemas de archivos NTFS. Como se puede observar, hemos pospuesto parte de la información sobre $AttrDef porque debemos explicar en primer lugar en qué consisten exactamente los atributos. Cada entrada en la MFT contiene información sobre los archivos, tal como hemos mencionado, pero conviene plantearse cómo se estructura dicha información. NTFS utiliza atributos que actúan como etiquetas que indican al sistema el tipo de datos que viene a continuación y cómo debe analizarlos. La apariencia básica de una entrada en la MFT es bastante sencilla:

- Cabecera de la entrada MFT (tamaño fijo de 48 ó 56 bytes)
- ID del atributo 1 (4 bytes)
- Tamaño del atributo 1 (4 bytes)
- Datos del atributo 1 (tamaño variable)
- ...
- ID del atributo N
- Tamaño del atributo N
- Datos del atributo N
- ID del atributo = EndOfEntry = 0xFFFFFFFF

Dichos IDs de los atributos son los que definen los datos a los que siguen, es decir, si se trata de un nombre de archivo, los atributos del archivo, un descriptor de seguridad, los contenidos del archivo, etc. Dicha información es la que contiene $AttrDef: una lista de atributos que se puede encontrar asociada a cualquier archivo y su "significado". Existen unos 16 atributos definidos en el estándar NTFS, siendo los más utilizados de entre ellos $STANDARD_INFORMATION (ID = 0x10), $FILE_NAME (ID = 0x30) y $DATA (ID = 0x80).

Concluyen aquí las nociones básicas de NTFS. Existen numerosos detalles que no hemos mencionado, pero no entraban dentro del objetivo de este artículo.

Explicación ampliada de los atributos

Cuando se observa el estándar NTFS y se comienza a pensar sobre la manera de ocultar datos en el mismo, una de las primeras ideas probablemente consistirá en alterar las definiciones de los atributos para desconcertar a las herramientas forenses que puede utilizar el examinador. Eso fue lo que intentamos en el laboratorio y los resultados fueron sorprendentes. Los cambios que realizamos en el archivo $AttrDef no alteraron la capacidad del sistema operativo de acceder al volumen, y el software de análisis forense tampoco experimentó problemas. El caso del software de análisis forense no resultaba tan extraño, ya que puede utilizar valores fijos (*hardcoded*) o disponer de algún tipo de "modo seguro de recuperación". Pero en cuanto al sistema operativo, resultaba evidente que no estaba siguiendo el estándar, por lo que decidimos averiguar por qué seguía funcionando.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Ejecutamos nuestras herramientas y, tras una primera observación del controlador ntfs.sys, descubrimos una función interesante llamada NtfsMountVolume(). Era obvio que si el sistema operativo necesitaba leer el archivo $AttrDef debía realizarlo al montar un nuevo volumen, por lo que el siguiente paso consistió en intentar encontrar un acceso a los "archivos especiales" como $Volume, $MFT, etc. Tras una ardua búsqueda por el código de inicialización y las comprobaciones de seguridad pudimos averiguar que accede a los archivos especiales utilizando no su nombre, sino su posición en la tabla MFT. Mediante NtfsOpenSystemFile(), el sistema operativo puede cargar archivos en función de su posición, por lo que resulta posible comprobar cómo abre primero el archivo 0 ($MFT), a continuación los números 1 ($MftMirr), 3 ($Volume), 2 ($LogFile), etc., pero no existía acceso al número 4 ($AttrDef), ni desde la función NtfsMountVolume() ni desde ninguna otra función. En las versiones recientes del controlador, se accede a $AttrDef pero no se analiza su contenido, por lo que el problema persiste.

Para comprobarlo, abrimos una imagen DD de un sistema NTFS y borramos el contenido de $AttrDef para a continuación montar la imagen DD modificada. No surgió ningún problema. Pudimos acceder a todo el contenido de los archivos y trabajamos con ese disco durante horas sin ningún problema. Por tanto, nuestra primera idea para encontrar un buen escondite había fracasado en parte. Seguimos estudiando el controlador de NTFS para observar cómo analizaba los atributos y descubrimos que en el propio controlador se encontraba una copia estática de los contenidos completos del archivo $AttrDef:

```
.data:00037900 ; Segment type: Pure data
.data:00037900 ; Segment permissions: Read/Write
.data:00037900 _data            segment para public 'DATA' use32
.data:00037900                  assume cs:_data
.data:00037900                  ;org 37900h
.data:00037900 _NtfsAttributeDefinitions:               ; DATA XREF: NtfsMountVolume+13D4↓o
.data:00037900                                          ; NtfsDeleteUcb(x,x)+25B↓o ...
.data:00037900                  unicode 0, <$STANDARD_INFORMATION>,0
.data:0003792C                  db 54h dup(0)
.data:00037980                  dd 10h                  ; Attribute ID
.data:00037984                  db 8 dup(0), 40h, 3 dup(0), 30h, 7 dup(0), 48h, 7 dup(0)
.data:000379A0 aAttribute_list_0:
.data:000379A0                  unicode 0, <$ATTRIBUTE_LIST>,0
.data:000379C0                  db 60h dup(0)
.data:00037A20                  dd 20h                  ; Attribute ID
.data:00037A24                  db 8 dup(0), 80h, 0Bh dup(0)
.data:00037A38                  align 10h
.data:00037A40 aFile_name:
.data:00037A40                  unicode 0, <$FILE_NAME>,0
.data:00037A56                  db 6Ah dup(0)
.data:00037AC0                  dd 30h                  ; Attribute ID
.data:00037AC4                  db 8 dup(0), 42h, 3 dup(0), 44h, 7 dup(0), 42h, 2, 6 dup(0)
.data:00037AE0 aObject_id:
.data:00037AE0                  unicode 0, <$OBJECT_ID>,0
.data:00037AF6                  db 6Ah dup(0)
.data:00037B60                  dd 40h                  ; Attribute ID
.data:00037B64                  db 8 dup(0), 40h, 0Ch dup(0), 1, 6 dup(0)
.data:00037B80 aSecurity_descriptor:
.data:00037B80                  unicode 0, <$SECURITY_DESCRIPTOR>,0
.data:00037BAA                  db 56h dup(0)
.data:00037C00                  dd 50h                  ; Attribute ID
.data:00037C04                  db 8 dup(0), 80h, 0Bh dup(0)
.data:00037C18                  align 10h
.data:00037C20 aVolume_name:
.data:00037C20                  unicode 0, <$VOLUME_NAME>,0
.data:00037C3A                  db 49h, 4Ch, 4Fh, 56h, 45h, 43h, 48h, 4Ch, 4Fh, 45h, 5Ch dup(0)
.data:00037C3A                  db 60h, 0Bh dup(0), 40h, 3 dup(0), 2, 8 dup(0), 1, 6 dup(0)
.data:00037CC0 aVolume_information:
```

Figura 1: contenido de $AttrDef *hardcoded* dentro del controlador ntfs.sys

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

El estándar NTFS permite a los programadores de software de terceros añadir nuevos atributos al sistema mediante ID de atributo mayores de 0x100. Desgraciadamente, dicha posibilidad no se encuentra documentada y no parece que exista ninguna interfaz con un sistema operativo que permita hacerlo sin un conocimiento profuso del sistema de archivos NTFS y un acceso al mismo en bruto.

Otra posibilidad consistía en utilizar un controlador modificado con una tabla de definiciones de atributos diferente, pero tampoco funcionó, debido a las diferentes comprobaciones (también estáticas) realizadas desde otras partes del sistema y el propio controlador.

Como paso final, decidimos codificar una mera prueba de concepto que simplemente almacena información cifrada dentro del archivo $AttrDef. El sistema operativo nunca analiza dicho archivo, ni lo modifica si no se vuelve a formatear el volumen. Además, nuestros datos están a salvo de cualquier búsqueda mediante el teclado y su almacenamiento pasará desapercibido para la mayoría de los examinadores forenses, puesto que $AttrDef no es precisamente un lugar habitual para buscar información. El punto débil reside, obviamente, en la detección de la herramienta utilizada para el acceso y el descifrado, pero esa es otra cuestión.

Ocultar archivos al software de análisis forense

Tras esta experiencia no demasiado buena con las estructuras hardcoded, pensamos que, si el sistema operativo no seguía el estándar NTFS, probablemente tampoco lo harían algunos programas informáticos de análisis forense, lo que conduciría a una interpretación diferente de los datos y permitiría a los usuarios malintencionados crear artefactos de NTFS extraños que confundieran a los investigadores.

Uno de los ensayos realizados fue parecido a la modificación de atributos que intentamos anteriormente pero utilizando la cabecera de la entrada de la MFT. Esta cabecera es una estructura compleja que contiene algunos números de secuencia y de referencia, indicadores que señalan si se trata de una entrada asignada o borrada, si se trata de un archivo o un directorio, etc. Nos centramos en los cuatro primeros bytes, que actúan como un número mágico, como PK para los archivos zip o MZ para los ejecutables. El valor más común para dichos bytes consiste en la secuencia ASCII "FILE", pero se permiten otros tres valores:

- **FILE**: entrada de archivo normal
- **CHKD**: entrada modificada por chkdsk (Check Disk)
- **BAAD**: entrada corrupta
- **HOLE**: desconocida

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Es evidente que si vemos "*unknown*" (desconocido) o "*undocumented*" (no documentado), debemos realizar una prueba de los mismos. En este experimento, elegimos un único archivo dentro de una imagen de NTFS y cambiamos de "FILE" a "HOLE". La imagen resultó ser bastante interesante, ya que el sistema operativo apreció la existencia de un archivo en ese lugar (aunque no nos permitió abrirlo) pero algunos de los programas informáticos de análisis forense probados ignoraron el archivo:

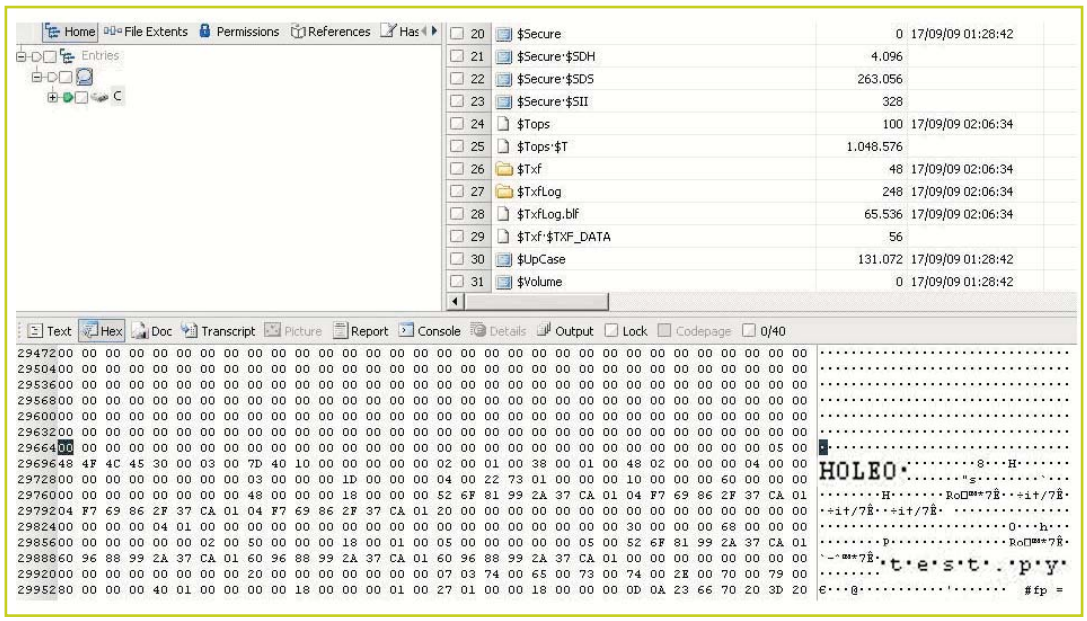

Figura 2: visualización de una imagen de NTFS elaborada a partir de EnCase. El archivo "test.py" no aparece en la vista de entradas.

Mostramos una captura de pantalla de EnCase porque Guidance Software solucionó este problema en EnCase 6.8 (he ahí una razón para actualizar el software de análisis forense). Dejamos como epropuesta al lector el realizar la misma prueba con otros softwares forenses.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Conclusiones

En este artículo hemos intentado mostrar el modo de enfocar la búsqueda de lugares en los que se puede esconder la información en los sistemas de archivos NTFS. Se trata de una manera interesante de aumentar nuestro conocimiento de NTFS y nuestra habilidad para identificar lugares en los que puede existir información oculta.

Los dos métodos anti forenses mostrados son bastante sencillos y (esperemos que) útiles para aquellos interesados en comenzar a investigar sobre el tema. Debe tenerse en cuenta que hemos realizado el análisis únicamente en una pequeña parte de la estructura del sistema de archivos NTFS, por lo que quedan numerosos lugares en los que puede ocultarse información. Por último, el hecho de que la implementación actual del controlador de NTFS no siga totalmente los estándares ofrece un pequeño campo de investigación de incoherencias entre las diferentes implementaciones y ayuda a recordarnos que las herramientas sirven únicamente para facilitar nuestra vida pero no debemos confiar ciegamente en ellas.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Editor de la Sección: Matías Bevilacqua

Esta sección se centrará en el aspecto técnico de la cibercriminalidad y las pruebas electrónicas. Se anima a los lectores a que contribuyan en esta sección. Dada la complejidad técnica del sistema de clasificación empleado, estamos abiertos a artículos divulgativos que sirvan de introducción a la tecnología, libros blancos innovadores, entre otros temas. Por favor, póngase en contacto con el editor si quiere colaborar en esta sección.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

DAVE CHILDS

Director de la Unidad de Recuperación de Prueba Electrónica · Oficina de Defensa del Consumidor de North Yorkshire, Reino Unido

EL USO DE LAS TECNOLOGÍAS VIRTUALES PARA EL ANÁLISIS DE LA PRUEBA ELECTRÓNICA

Dave Childs es director del laboratorio de recuperación de prueba electrónica y de delitos a través de Internet de la Oficina de Defensa del Consumidor de North Yorkshire desde julio de 2006. Gran parte de su labor está relacionada con la investigación de delitos comerciales, como la falsificación, aunque también realiza trabajos por cuenta de algunos cuerpos policiales locales.

Antes de desempeñar este cargo, fue el primer civil contratado como analista de informática forense por la policía de North Yorkshire, tarea para la que aprovechó su experiencia anterior como agente de policía en las policías de North Yorkshire y Staffordshire.

Ha obtenido recientemente un título de postgrado en técnicas forenses aplicadas a la ciberdelincuencia, creado gracias a una iniciativa conjunta de la Agencia Nacional de Mejora de la Policía del Reino Unido y la Universidad Canterbury Christ Church.

La disciplina de la técnica forense aplicada a la ciberdelincuencia engloba diversas funciones con distintos grados de responsabilidad. Estas funciones no siempre están definidas claramente, sino que pueden variar entre las diferentes organizaciones, y algunos profesionales pueden ser responsables de más de una función en su lugar de trabajo. Kipper[1] divide estas funciones en las siguientes:

1. El primer interventor, es decir, la persona que acude al lugar del delito y es responsable de la incautación de elementos constitutivos de prueba electrónica.
2. El técnico, que puede ser responsable de la recepción y la manipulación de los objetos probatorios, así como de la adquisición de imágenes forenses a partir de soportes digitales.
3. El examinador forense, que utiliza software y hardware especializados para recuperar los datos digitales.
4. El analista forense, que evalúa los datos de los examinadores y valora la relevancia de dichos datos para la investigación en curso.

El analista de informática forense no suele ser el agente encargado de una investigación completa, sino desempeña más bien la función de especialista dentro de la investigación general, concretamente para el análisis de la prueba electrónica. El agente al cargo, es decir, aquel que se ocupa de la investigación, normalmente es responsable de la fase inicial de recopilación de pruebas, incluida la incautación de pruebas electrónicas, así como del interrogatorio

* Idioma original del artículo: Inglés. El artículo original se puede encontrar en la versión inglesa del ENAC.
[1] Kipper, G. (2007) *Wireless Crime and Forensic Investigation.* Boca Raton: Auerbach Publications.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

de los posibles testigos y sospechosos. Dicho agente enviará los dispositivos digitales incautados al analista forense, acompañados normalmente de un impreso de envío que proporciona información detallada acerca de la investigación, indicando qué información resulta necesaria para el análisis.

Algunos aspectos del proceso de la informática forense son comunes a la mayoría de las investigaciones:

1.La preparación, que incluye aspectos como el examen físico, un inventario del hardware y una comprobación de la configuración de la BIOS.
2.La adquisición de imágenes forenses a partir de los datos almacenados dentro de los objetos probatorios.
3.Procesos preliminares mediante el software de informática forense, como la recuperación de archivos y carpetas borrados, el montaje de archivos, el análisis de la firma de archivos, el cálculo de los valores hash de archivos y la recuperación de archivos borrados. Los procesos que se ejecutan dependen de las necesidades del análisis y de las preferencias del analista.

Sin embargo, todos estos procesos preliminares se llevan a cabo para preparar la fase en la que se identifican los datos con importancia probatoria. Este aspecto del proceso difiere de los anteriores en que no siempre requiere el conocimiento especializado de personal con formación en técnicas forenses, sino más bien las competencias de un investigador.

En algunas investigaciones, como en las derivadas de la posesión de imágenes obscenas de niños, o en los delitos específicamente relacionados con ordenadores, como el abuso informático, es posible que el analista de informática forense sea responsable de la aportación de la mayoría de la prueba que fundamente la investigación, puesto que la prueba electrónica constituirá el área que presente mayores probabilidades de contener material importante. No obstante, incluso algunos aspectos de estos tipos de investigaciones, como la identificación de la ilicitud de las imágenes contenidas en los objetos probatorios, no requieren conocimientos en informática forense y no es necesario que se encargue de ellos técnico.

En otros casos, la investigación puede requerir la identificación de prueba en forma de texto, como, por ejemplo, documentos o correo electrónico. En estos casos, los documentos probatorios pueden resultar obvios, pero es posible que existan datos relevantes que pasen desapercibidos para aquellos que no participen en la propia investigación. Un ejemplo de esto puede consistir en la presencia de correos electrónicos entre los sospechosos y un tercero cuyo contenido no parezca relevante. Sin embargo, el mero hecho de que estas personas mantengan una relación puede revestir una gran importancia. Dicha conexión únicamente puede ser percibida por alguien que pueda valorar los datos basándose en el conocimiento de otros elementos de la investigación. Durante esta fase, los datos digitales deben presentarse a un agente no especialista para su análisis, lo que, en la actualidad, implica a menudo su desplazamiento al lugar de trabajo del analista forense y la utilización de todo el software de informática forense o una versión limitada del mismo.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Mientras que esto puede resultar eficaz en aquellos casos en los que los archivos probatorios puedan identificarse fácilmente y exista un número relativamente pequeño de los mismos, pueden darse otros casos en los que el agente al cargo precise un periodo de tiempo largo para analizar la prueba. Un ejemplo de lo anterior es el de las investigaciones que requieran el análisis de archivos financieros relacionados con estafa, localización de bienes o investigaciones de delitos financieros.

Otro problema relacionado con el uso del software de informática forense para el análisis de archivos de datos surge cuando estos se encuentran en un formato que únicamente permite la visualización de la información mediante el software utilizado para crearlos. Esto ocurre, por ejemplo, con los archivos de datos creados mediante el software de contabilidad Sage Line 50[2]. Los datos creados mediante este software se almacenan utilizando una estructura de archivos propia y se presentan a partir de diversos archivos diferentes. La única forma de visualizar correctamente estos datos pasa por el uso del propio software Line 50.

Para que los agentes al cargo puedan disponer de acceso a dichas pruebas, deben identificarse nuevos métodos para presentarlas en un formato que aquellos puedan utilizar en su propio entorno de trabajo. Para poner en marcha estos métodos, debe confirmarse que:

1. se mantenga la integridad de los archivos probatorios;
2. la cantidad de datos probatorios se corresponda con la disponible en las herramientas forenses que se utilicen en ese momento; y
3. todo dato probatorio identificado resulte fiable a efectos de los posteriores procedimientos judiciales.

El uso de tecnología virtual

Un método utilizado para sobreponerse a dichas dificultades dentro del laboratorio forense consiste en el uso de la tecnología de máquina virtual. Este proceso implica normalmente el montaje de una imagen forense creada desde el ordenador que va a examinarse y el uso de software, como VMWare Workstation[3] o Microsoft VirtualPC[4] para crear una máquina virtual que contenga todo el sistema operativo del equipo original, así como el software instalado en el mismo y sus archivos de datos. Una vez creada dicha máquina virtual, pueden visualizarse los datos que deben analizarse dentro de su paquete de software nativo. Los datos interesantes pueden exportarse del software original, si se dispone de dicha función, o puede realizarse una captura de pantalla de los datos relevantes dentro del software.

La desventaja de dichos métodos reside en la portabilidad de la prueba: para visualizar las máquinas virtuales creadas de esta manera, deben proporcionarse las imágenes forenses originales, o las copias clonadas de los discos duros, junto con el software necesario para ejecutar la máquina virtual. Los ordenadores domésticos medios se comercializan actualmente con una capacidad de almacenamiento en disco duro de entre 100 y 500 GB, las

[3] VMWare Inc. (2008) VMware: virtualización, máquina virtual y consolidación de servidores virtuales – VMware. Disponible en: http://www.vmware.com/
[4] Microsoft Corporation. (2008d) http://www.microsoft.com/windows/virtual-pc/default.aspx
Disponible en: http://www.microsoft.com/windows/virtual-pc/default.aspx

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

imágenes forenses presentan normalmente un tamaño de entre 50 y 250 GB, y las unidades clonadas se corresponderán en tamaño con el de las unidades originales. Dichas cuestiones de almacenamiento presentan repercusiones económicas, ya que es necesario almacenar grandes cantidades de datos en un soporte portátil.

Un uso alternativo de la tecnología de máquina virtual consiste en crear una máquina virtual mediante una instalación nueva de un sistema operativo junto con una instalación nueva del paquete de software utilizado para crear los archivos de datos que deben analizarse. De este modo, los archivos de datos sospechosos pueden transferirse a esta máquina virtual y examinarse utilizando el software original. La ventaja de este método sobre los detallados anteriormente radica en que la máquina virtual solo necesita ser lo suficientemente grande como para dar cabida al sistema operativo, a los archivos de datos sospechosos y a su paquete de software original. De esta forma, es posible que únicamente resulte necesaria una máquina virtual de unos pocos gigabytes en lugar de una que utilice un disco o una imagen forense de varios cientos de gigabytes, por lo que aumentan las opciones de soporte portátil, pudiendo utilizarse discos ópticos o dispositivos de almacenamiento USB.

Se ha llevado a cabo una comparación de las respectivas ventajas que ofrecen tres paquetes de software de máquina virtual a la hora de crear una máquina virtual para su uso en la investigación de archivos de datos. El software utilizado fue VMWare Workstation y Microsoft VirtualPC para la plataforma Windows, y el software QEMU Bellard, F. (2008) QEMU[5] para Linux. En cada uno de los casos, se creó una máquina virtual con una nueva instalación de Windows XP y, en cada una de las máquinas virtuales, se instaló el software de contabilidad Sage Line 50. A continuación, se copiaron los archivos de datos del ensayo en las máquinas virtuales y se examinaron los datos dentro del software original. Aunque el software utilizado para crear la máquina virtual fue diferente en cada caso, se probó cada máquina virtual mediante el software gratuito VMWare Player[6], disponible tanto en versión Windows como Linux.

Al utilizar las máquinas virtuales de esta manera, los archivos de datos resultan fácilmente comprensibles desde el software original, mientras que los mismos datos son prácticamente imposibles de interpretar cuando se visualizan como datos en bruto en software de informática forense. Un análisis de los valores hash de los archivos confirman que los datos son precisos y que no se han alterado, incluso después de haberse visualizado en la máquina virtual. Sin embargo, este uso de las máquinas virtuales genera el problema de que no pueden ejecutarse en modo de solo lectura, ya que VMWare Player requiere un acceso de lectura y escritura a la máquina virtual y al soporte desde el que se ejecuta. Esto significa que la persona que analiza los datos debe estar al corriente de que todo cambio que realice se guardará y puede afectar a otros datos de la máquina virtual. Para solucionar este problema, en algunos programas de software de máquina virtual es posible descartar los cambios realizados en la máquina virtual al finalizar la sesión de usuario, aunque esta opción no se encuentra disponible en el software VMWare Player.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

[5] Bellard, F. (2008) QEMU. Disponible en: http://bellard.org/qemu/
[6] VMWare Inc. (2009) VMware Player - Utilice varios sistemas operativos mediante la descarga gratuita de VMware - VMware. Disponible en: http://www.vmware.com/products/player/

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Método de entrega

Además de llevar a cabo una comparación de las tecnologías de máquina virtual, se ha realizado también un análisis de los métodos disponibles para suministrar las máquinas virtuales al usuario final. Las opciones examinadas fueron el uso de pendrives USB, discos duros externos y DVD grabables. Para evaluar la eficacia del soporte potencial, se otorgó especial importancia a las posibles limitaciones que podría encontrar el usuario final al intentar utilizar la máquina virtual en una estación de trabajo conectada en red, ya que, a menudo, en las organizaciones grandes el usuario no puede instalar software ni ejecutar paquetes de software que requieran permiso de escritura en el registro local.

Las soluciones examinadas para la entrega de las máquinas virtuales fueron las siguientes:

·Suministrar la máquina virtual junto con el software VMWare Player o el software de instalación de VirtualPC en un soporte extraíble. El principal problema de esta solución radica en la necesidad de instalar cualquiera de los dos paquetes de software en el equipo local antes de poder utilizarse, lo que puede impedir su uso en redes con restricciones. Si no existen dichas restricciones, cualquiera de las dos soluciones es satisfactoria, presentando VirtualPC la ventaja añadida de poder descartar los cambios introducidos por el usuario al final de la sesión.
·Usar un sistema operativo portátil, como MojoPac[7], que puede guardarse en un pendrive USB y utilizarse en varios ordenadores. En esta solución, el usuario no crea una máquina virtual autónoma, sino que instala el software que debe utilizarse para examinar los datos sospechosos en la sesión de MojoPac y copia los archivos de datos en el mismo. MojoPac presenta problemas para instalar el software en el equipo local y también para instalar el software en MojoPac, ya que, a menudo, se tardan horas en instalar un paquete que se instala en tan solo unos minutos en las versiones estándar del sistema operativo Windows. Una vez instalado el software, la solución MojoPac es eficaz, aunque no dispone de función de "instantánea", por lo que el usuario final debe saber que todo cambio que realice será permanente.
·Crear un Live DVD de Linux que incluya la máquina virtual y que permita al usuario final iniciar el sistema operativo Linux desde una estación de trabajo en una red con restricciones, superando así toda restricción de uso impuesta a su cuenta de usuario. Un problema de este método consiste en que la creación inicial del Live DVD de Linux es bastante compleja y requiere el conocimiento del sistema operativo Linux y de una distribución Linux de trabajo. Otro problema radica en que el software VMWare Player requiere acceso de lectura y escritura a la ubicación en que se almacenan los archivos de la máquina virtual, por lo que, aunque el usuario puede iniciar el sistema operativo Linux, no puede ejecutar la máquina virtual guardada en el DVD del software Player. Esta solución puede utilizarse si los archivos de la máquina virtual se guardan en un pendrive USB que se introduzca en la sesión Live de Linux que se esté ejecutando.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

[7] RingCube Technologies, I. (2008) MojoPac. Disponible en: http://www.mojopac.com/download.html

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

·Crear un Live pendrive USB de Linux, que presenta la ventaja de evitar el sistema operativo huésped y que permite también que VMWare Player disponga de acceso con permiso de escritura a la máquina virtual. Se puede crear fácilmente el Live pendrive desde una instalación de Windows XP mediante un archivo de procesamiento por lotes descargado del sitio web Pen Drive Linux[8] y, una vez logrado, se pueden evitar las restricciones del equipo en red y es posible ejecutar la máquina virtual sin problemas.

Al utilizar las máquinas virtuales de esta manera, pueden surgir problemas de licencia del software, por lo que la persona que cree la máquina virtual deberá asegurarse de que el sistema operativo y todos los paquetes de software incluidos dispongan de la licencia adecuada o que se hayan obtenido las exenciones pertinentes del propietario de la licencia.

Si se identifican datos por cualquiera de estos métodos y posteriormente deben servir como prueba en cualquier procedimiento, el investigador debe adoptar las medidas necesarias para confirmar la validez de los datos. Esto puede realizarse mediante la comprobación por el analista forense de que los datos están presenten en la imagen forense original y coinciden con los mismos.

Conclusiones

Los investigadores sin formación en informática forense experimentan una necesidad creciente de disponer de un acceso prolongado a las pruebas electrónicas. A menudo, no les resulta práctico desplazarse en repetidas ocasiones hasta sus instalaciones de informática forense, por lo que deben idearse nuevos métodos para que puedan recopilarse y visualizarse los datos en un formato comprensible en la propia estación de trabajo del investigador. Una de las maneras en que esto puede lograrse es por medio de las tecnologías virtuales, que permiten entregar al investigador soportes portátiles que contienen los datos que deben analizarse dentro de una máquina virtual que también incluye el software original utilizado para crear los datos.

Para garantizar la posibilidad de utilizar la máquina virtual en una estación de trabajo que puede estar conectada a una red con restricciones, es posible suministrarla como parte de una distribución Live de Linux, capaz de evitar el sistema operativo instalado. Sin embargo, la propia máquina virtual debe almacenarse en un soporte grabable. Como solución a este problema, en la mayoría de las situaciones servirá el uso de una distribución Live de Linux en un pendrive USB.

El uso de máquinas virtuales de este modo puede resultar muy útil para la investigación de las pruebas electrónicas. Sin embargo, dicho análisis debe llevarse a cabo sabiendo que la alteración de los datos por el investigador puede arrojar resultados imprecisos. Por esta razón, toda información valiosa debe compararse con los datos originales en poder del analista forense.

[8] Pen Drive Linux. (2009) Crea tu propia distribución Live CD o USB de Linux | USB Pen Drive Linux. Disponible en: http://debian-live.alioth.debian.org/

Editor de la Sección: Nigel Jones

El objetivo de esta sección del ENAC es ofrecer la información más actualizada a nivel internacional en lo referente al cumplimiento de la ley en la cibercriminalidad y en la informática forense. Esto solo se puede conseguir si la gente está dispuesta a colaborar con artículos de interés. Reconocemos que las investigaciones implican técnicas sensitivas, y no esperamos que se revele información detalla. Obtener información de asuntos específicos, especialmente si afectan fuera de las fronteras, puede ser interesante y beneficiar a nuestros lectores. Si existe algún tema de interés sobre el que quiera escribir un artículo o, que le hagamos una entrevista, póngase en contacto con el editor de la sección.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company


RADOMÍR JANSKÝ y RUBEN LOMBAERT

Dirección F.2 de lucha contra la delincuencia organizada de la Dirección General de Justicia, Libertad y Seguridad · Comisión Europea

HACIA UNA ESTRATEGIA EUROPEA UNIFICADA PARA COMBATIR LA CIBERDELINCUENCIA

El Dr. Radomír Janský es responsable de asuntos relativos a la ciberdelincuencia en la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea. Antes de ocupar este puesto en la Comisión, trabajó como asistente parlamentario en el Parlamento Europeo, desempeñando su trabajo en la Comisión de Relaciones Exteriores. Se doctoró en Política en el Nuffield College de la Universidad de Oxford. También ostenta títulos de postgrado en Ciencias Políticas y Económicas en universidades del Reino Unido (Oxford), Hungría (Universidad Centroeuropea) y la República Checa (Universidad de Bohemia Occidental).

Ruben Lombaert trabaja actualmente como responsable de políticas en la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea, donde está encargado de la ciberdelincuencia. Antes de desempeñar este puesto en la Comisión Europea, fue miembro del personal académico del Instituto de Estudios Europeos de la VUB (Vrije Universiteit Brussel, en Bélgica), donde fue responsable de la formación online. Estudió Ciencias Políticas y Asuntos Europeos en la Universidad de Gante (Bélgica), el Colegio de Europa, la Universidad de Oxford (Reino Unido) y la Universidad de Grenoble (Francia).

El avance de los sistemas electrónicos de información modernos ha generado importantes efectos beneficiosos en nuestras sociedades, pero, al mismo tiempo, ha provocado una progresiva dependencia de dichos sistemas. Esto ha traído consigo riesgos considerables para los ciudadanos, las empresas y las administraciones públicas. La **ciberdelincuencia**, esto es, las actividades delictivas en forma de ataque contra los sistemas de información o de delitos más tradicionales, como la estafa y la difusión de material con contenido que revele abuso o agresión sexual a menores, cometidas por medio de sistemas de información, constituye un problema creciente en Europa y el resto del mundo. Los recientes ataques contra la infraestructura de información crítica de Estonia y el aumento de la cantidad de material con contenido revelador de abuso o agresión sexual a menores disponible en Internet subrayan la urgencia de la necesidad de actuación contra este nuevo tipo de delincuencia.

* Idioma original del artículo: Inglés. El artículo original se puede encontrar en la versión inglesa del ENAC.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

La ciberdelincuencia cruza a menudo las fronteras en una fracción de segundo y afecta a varios países al mismo tiempo. Desde el punto de vista de las ejecución de la ley, esto plantea problemas, como la determinación de la jurisdicción competente, la decisión sobre qué ley resulta aplicable, la ejecución de la ley a nivel transfronterizo, y el reconocimiento y uso de la prueba electrónica. Resulta evidente que para combatir la ciberdelincuencia es necesaria una mayor cooperación internacional, ya que ninguna política sobre la ciberdelincuencia puede ser eficaz si su aplicación queda confinada a las fronteras de los diferentes países.

El énfasis en la cooperación internacional a nivel mundial no menoscaba la importancia de la **cooperación a nivel de la UE**, sino más bien al contrario, ya que la elaboración de una estrategia europea unificada para luchar contra la ciberdelincuencia es esencial si Europa desea contribuir de una manera más eficaz a los esfuerzos realizados a nivel mundial para combatir la ciberdelincuencia. Además, una estrategia común contra la ciberdelincuencia seguramente reforzaría de forma global la construcción del espacio europeo común de justicia, libertad y seguridad.

Durante varios años, la Comisión ha elaborado una estrategia europea coherente para luchar contra la ciberdelincuencia en cooperación con los Estados miembros de la UE y otras instituciones de la UE e internacionales. En una comunicación de la Comisión, *"Towards a general strategy on the fight against cyber crime"* (Hacia una estrategia general en la lucha contra la ciberdelincuencia), de mayo de 2007, se presentaron varios pasos importantes para la formulación de la estrategia. Se pueden distinguir tres áreas de actividad principales: legislación, ejecución de la ley a nivel transfronterizo y colaboración entre los sectores público y privado.

El primer campo consiste en las medidas legislativas adoptadas. Para ello, se controla de cerca la legislación nacional en este ámbito, con el objetivo a largo plazo de lograr cierto grado de acercamiento en el derecho penal pertinente. Este acercamiento es deseable para evitar vacíos en los ordenamientos jurídicos de los Estados miembros que puedan obstaculizar la respuesta contra la ciberdelincuencia a nivel nacional por parte de las Fuerzas y Cuerpos de Seguridad, así como de las autoridades judiciales. Con el tiempo, esto debe conducir, además, a un mayor grado de cooperación internacional. Cuando se trata de la toma de decisiones a nivel de la UE, el derecho de iniciativa (legislativa) en asuntos relacionados con la justicia y los asuntos de interior se encuentra compartido entre la Comisión y los Estados miembros, siendo generalmente necesario el voto unánime del Consejo. Deben mencionarse dos importantes documentos legislativos existentes en materia de ciberdelincuencia: la Decisión Marco 2005/222/JAI del Consejo relativa a los ataques contra los sistemas de información y la Decisión Marco 2004/68/JAI del Consejo relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil. La Comisión propuso recientemente la actualización de la última para que tuviera e cuenta las nuevas formas de abuso y agresión sexual de menores, especialmente *online*[1]. También se está preparando la actualización de la Decisión Marco 2005/222/JAI del Consejo para poder combatir de forma más eficaz los ataques cibernéticos a gran escala, que constituyen a día de hoy la principal amenaza para nuestros sistemas de información.

[1] COM(2009)135 final

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Ambos documentos legislativos garantizan un nivel mínimo de acercamiento del derecho penal en lo que respecta a las formas más importantes de las actividades delictivas reguladas en los mismos, como los ataques cibernéticos y la pornografía infantil, respectivamente.

En segundo lugar, la Comisión promueve activamente el desarrollo de la **cooperación transfronteriza entre las Fuerzas y Cuerpos de Seguridad dentro de la UE**. Los delitos informáticos no solo presentan un carácter internacional sino que también se cometen de una manera extremadamente rápida. Por tanto, es importante que se pueda actuar rápidamente a nivel transfronterizo para poder detener a los delincuentes, que pueden desplazarse a gran velocidad a través de las fronteras. Para ello, es esencial que se estrechen las relaciones entre los expertos en ciberdelincuencia de los diferentes Estados miembros, y la Comisión apoya este proceso por medio de diversas medidas incluidas en las políticas. Entre estas medidas se encuentran el refuerzo de las personas de contacto de los Estados miembros para la cooperación internacional, la elaboración de una plataforma a nivel de la UE para la formación en la investigación de la ciberdelincuencia y la asistencia para el intercambio de prácticas recomendadas en toda la UE. Para promover el intercambio de información y facilitar las investigaciones conjuntas sobre ciberdelincuencia, se está creando en Europol una plataforma europea de alerta sobre delitos relacionados con Internet gracias al apoyo financiero de la Comisión.

En tercer lugar, la Comisión promueve la cooperación entre los cuerpos policiales y los operadores privados para la lucha contra la ciberdelincuencia en la UE y fuera de sus fronteras. La **colaboración entre los sectores público y privado** constituye un elemento fundamental de toda política integral contra la ciberdelincuencia. Toma la forma de intercambio de información, prácticas recomendadas, formación y solicitudes de asistencia. La Comisión celebra reuniones periódicas con especialistas de los sectores público y privado para examinar los medios de consolidación de la cooperación en la UE. Con este fin, primero los expertos, en septiembre de 2008, y posteriormente el Consejo de la Unión Europea, en noviembre de 2008, aprobaron unas propuestas específicas[2]. Una de ellas trata de la formación en la investigación de la ciberdelincuencia. Esta resulta aplicable tanto a los sectores público como privado y, tal como se ha indicado anteriormente, la Comisión está creando una plataforma europea de formación, conjuntamente con los Estados miembros, Europol, CEPOL, las universidades y el sector privado.

Otra importante iniciativa público-privada consiste en la Coalición Financiera Europea contra la distribución comercial de imágenes de abusos sexuales de menores en Internet, que se puso en marcha en marzo de 2009. No cabe ninguna duda de que la fuerza motriz que impulsa la distribución de pornografía infantil, quizá más que en el resto del mundo, es el beneficio económico que puede lograrse. Actuando contra dichos beneficios económicos podremos evitar muchos casos de abusos en el futuro. El objetivo de la "Coalición Financiera" es el de combinar el trabajo de las diferentes partes, públicas o privadas, involucradas para combatir la producción, la distribución y la venta de imágenes de pornografía infantil en Internet, garantizando que el lucro económico resulte más difícil al mismo tiempo que se localizan y arrestan los delincuentes que participen en dichas actividades.

[2] Diario Oficial de las Comunidades Europeas, C 62, 17.3.2009, p. 18.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Los participantes en esta coalición son los principales proveedores de servicios de Internet, los bancos y proveedores de sistemas de pago, las ONG, las compañías telefónicas, las empresas de TI, los organismos públicos, las organizaciones internacionales (Europol y Eurojust), los cuerpos policiales y las autoridades judiciales.

Últimamente, la Comisión ha puesto en marcha también diversos **programas financieros**, que apoyan su estrategia y sus actividades en colaboración con los socios antes mencionados. Entre los mismos, podemos citar a modo de ejemplo los programas "Prevención y lucha contra la delincuencia" y "Para una Internet más segura". En su mayor parte, se trata de subvenciones que pueden solicitar las administraciones públicas, las ONG y el sector privado.

No cabe duda de que las acciones descritas anteriormente son tan solo el comienzo de una internacionalización en la lucha contra la delincuencia, que comienza a nivel de la UE. Pero esta lucha también debe estar orientada por una visión de futuro, dada la espectacular velocidad con la que avanzan las técnicas de la ciberdelincuencia. La Comisión expuso recientemente su visión en un **nuevo programa multianual** llamado "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos"[3]. La nueva estrategia propuesta reconoce que la economía digital constituye un importante factor de crecimiento y que la Unión Europea debe promover políticas que garanticen un nivel muy alto de seguridad en la red. Por tanto, la Unión Europea debe aclarar las normas sobre la jurisdicción y el marco jurídico aplicable al ciberespacio para promover las investigaciones transfronterizas y hacer de Internet una fuerza motriz de los futuros desarrollos económico y social, aspectos todos ellos a los que espera contribuir la Comisión.

Para una mayor información, véase:
http://ec.europa.eu/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm (en inglés)

[3] COM(2009)262 final

Editor de la Sección: Liljana Selinšek

Invitamos al lector a que se ponga en contacto con la editora si quiere presentar las actividades de su Institución en la lucha contra el cibercrimen.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Los casos resumidos a continuación en este número recogen un conjunto diverso de aspectos sobre la prueba electrónica que pueden plantearse en tribunales de todo el mundo, e incluyen una acción que prosperó en China cuya base consistía en el suministro ilícito de software, el problema de las autoridades encargadas de la instrucción para obtener la contraseña de un sospechoso en EE. UU., la realización de notificaciones a través de Internet en Australia y la determinación de la autenticidad de la prueba electrónica en la India. Como aspecto interesante, se sugiere que los dos casos de Australia no son incompatibles. Aunque puede pensarse que los comentarios del magistrado Ryrie son, en cierto modo, escépticos, su decisión es correcta debido a la ausencia de una mayor prueba de la identidad. Por su parte, la decisión del magistrado Harper de realizar una notificación poniéndose en contacto con los demandados a través de la página de Internet Facebook como uno de los medios posibles de notificación de los documentos a los demandados es correcta, ya que, en caso contrario, los demandados podrían llegar a la conclusión de que pueden eludir los efectos de sus acciones. En el caso conocido por el magistrado Harper, el demandante presentó prueba suficiente como para demostrar que las personas que aparecían en Facebook eran las mismas que aquellas a las que se intentaba notificar de la sentencia en rebeldía.

País: Australia
Citación del caso: Citigroup Pty Ltd contra Weerakoon [2008] QDC 174 (16 de abril de 2008)
Nombre y grado del tribunal: Tribunal del Distrito de Queensland

Escrito de demanda · notificación · Facebook

• SUMARIO

Se solicitó la notificación de los demandados a través de Facebook. En este caso, el magistrado Ryrie denegó el permiso para la notificación indirecta de un escrito de demanda mediante envío de correo electrónico a la página de Facebook del demandado. Esta decisión se fundamentó en la "incertidumbre de la página de Facebook", en que "cualquiera puede crear una identidad que simule la identidad de la verdadera persona" y en el hecho de que el magistrado no quedó convencido de que el autor de la página de Facebook se correspondiera con el demandado, aunque hizo constar que existían probabilidades de que esto fuera así.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

País: India
Citación del caso: el Estado contra Navjot Sandhu, alias Afsan Guru, y otros (2005), 11 SCC 600
Nombre y grado del tribunal: Tribunal Supremo

Registros de llamadas telefónicas · prueba · autenticidad

• SUMARIO

Se trata de una demanda que se interpone en relación con los procesos que siguieron al ataque al Parlamento Indio en diciembre de 2001. La sentencia contiene 195 páginas y desarrolla con gran detalle los fundamentos de la demanda. Este informe únicamente examina la autenticidad de ciertos registros de telefonía móvil.

El demandante alegó que no se constató adecuadamente la autenticidad de los registros relativos a las llamadas realizadas desde teléfonos móviles. Se argumentó que, en virtud de lo dispuesto en la Ley sobre Prueba de la India, resultaba necesario un certificado de fiabilidad, y que no podían admitirse las pruebas secundarias.

Se señaló que se citó a juicio a testigos para probar las impresiones de los registros digitales proporcionados por los operadores de telefonía móvil. Sin embargo, la prueba se aportó en forma de cartas, una firmada por el coordinador de Sterling Cellular Limited y la segunda firmada por el director de seguridad de Bharti Cellular Limited. Los miembros del Tribunal de Apelación encontraron relevante el hecho de que ninguno de los testigos fue cuestionado por la defensa en relación con la autenticidad de los registros en el juicio. Los argumentos ante el Tribunal Supremo se fundamentaron en la posibilidad de que los registros se hubieran falsificado. El Tribunal estimó que, puesto que no podían presentarse los servidores ante el Tribunal, únicamente podían aceptarse como prueba las impresiones, y que la parte actora era responsable de recabar las pruebas necesarias, junto con los certificados de fiabilidad pertinentes, para garantizar que las impresiones presentadas al tribunal durante el juicio fueran auténticas.

La parte actora admitió que los testigos no eran especialistas técnicos familiarizados con el funcionamiento de los ordenadores, pero los miembros del Tribunal Supremo consideraron irrelevante la falta de formación de los testigos en la materia. Se estimó que la prueba contenida en las impresiones indicaba claramente que los ordenadores funcionaban correctamente. Además, no parecía existir ningún tipo de manipulación ni defecto material de los ordenadores, debido a que existían errores en las impresiones que fueron corregidas automáticamente por el ordenador. Sobre este asunto concreto, el Tribunal llegó a la conclusión, en la página 716, de que era "legítimo presuponer que el sistema funcionaba correctamente y que los datos fueron producidos por el ordenador durante un uso normal del mismo, tanto si este hecho fue declarado expresamente por el testigo como si no".

El Tribunal concluyó que los registros telefónicos resultaban admisibles y fiables, y que la parte actora hizo un uso correcto de los mismos durante el juicio.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

País: Estados Unidos
Citación del caso: In re Boucher, 2007 WL 424473 (29 de noviembre de 2007); 2009 WL 424718, D.Vt., 19 de febrero de 2009
Nombre y grado del Tribunal: Tribunal de Distrito de Estados Unidos para el Distrito de Vermont

Archivos cifrados · autoincriminación · Quinta Enmienda

SUMARIO

En diciembre de 2006, Boucher y su padre atravesaron la frontera canadiense para entrar en Estados Unidos. En el asiento trasero de su coche llevaban un ordenador portátil. Un agente de policía cogió el ordenador, lo encendió y miró los archivos sin introducir ninguna contraseña. El agente buscó imágenes o vídeos en los archivos del ordenador. Este albergaba aproximadamente 40.000 imágenes, algunas de las cuales presentaban un nombre que sugería el carácter pornográfico de las mismas. Algunos nombres de archivos parecían indicar que la imagen podía contener pornografía infantil. Se llamó a un agente especial de la Policía de Inmigración y Aduanas, quien inspeccionó a continuación el ordenador. Encontró un archivo llamado "2yo getting raped during diaper change" (violación de niño de dos años durante el cambio de pañales). Se descubrieron miles de imágenes de pornografía con adultos y animaciones que mostraban pornografía con adultos e infantil.

Se solicitó a Boucher que abandonara la sala y el agente continuó examinando el ordenador, incluida la unidad Z, que Boucher había mostrado al agente. En la unidad Z encontró varias imágenes y varios vídeos de pornografía infantil. Se procedió al arresto de Boucher y a la incautación del ordenador, tras su apagado.

La policía creó una imagen de espejo del contenido del ordenador portátil. Cuando el especialista en prueba electrónica comenzó a examinar el ordenador, advirtió que no disponía de acceso a la unidad Z porque se encontraba protegida mediante cifrado, es decir, se necesitaba una contraseña para disponer de acceso a la unidad Z. Según el gobierno, el proceso de desbloqueo de la unidad Z podía llevar años, tomando como base los esfuerzos realizados en otro caso por desbloquear archivos cifrados de la misma manera. A pesar de intentarlo por todos los medios, el gobierno no pudo encontrar la contraseña necesaria para poder acceder a la unidad Z.

Para lograr acceso a la unidad Z y a los archivos en cuestión, el gran jurado citó a Boucher y le ordenó proporcionar todos los documentos, en formato electrónico o papel, que reflejaran las contraseñas utilizadas o asociadas con el ordenador portátil. Boucher solicitó la anulación de la citación alegando violación de su derecho a no autoincriminarse, recogido por la Quinta Enmienda. La moción de anulación de la citación fue concedida por el juez de primera instancia Jerome J. Niedermeier, fundamentando su decisión en el hecho de que revelar la frase de contraseña constituiría una forma de autoincriminación.

El gobierno recurrió la decisión del juez de primera instancia ante el magistrado de distrito encargado de su supervisión. Sin embargo, el gobierno también restringió su solicitud, ya que no solicitó la contraseña del disco duro cifrado, sino únicamente que Boucher mostrara el contenido de su disco duro cifrado en formato no cifrado mediante la apertura del disco ante el gran jurado. El magistrado del Tribunal de Distrito de Estados Unidos ordenó a Boucher que proporcionara al gran jurado una versión no cifrada del disco duro tal como lo vio el agente.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

País: Australia
Citación del caso: MKM Capital Property Limited contra Corbo y Poyser (n.º SC 608 de 2008, sin comparecencia, Tribunal Supremo del Territorio de la Capital Australiana, magistrado Harper, 12 de diciembre de 2008)
Nombre y grado del tribunal: Tribunal Supremo del Territorio de la Capital Australiana

Sentencia en rebeldía · notificación · Facebook

- SUMARIO

Doña Corbo y Don Poyser, demandados, obtuvieron dinero prestado del demandante para refinanciar la hipoteca de su vivienda. No realizaron los reembolsos cuando procedía, por lo que MKM emprendió acciones legales y obtuvo una sentencia en rebeldía por la cantidad del préstamo y la posesión de la vivienda de los demandados. MKM realizó una serie de intentos por notificar la sentencia en rebeldía, pero no pudieron localizarse los demandados. MKM solicitó posteriormente al Tribunal una orden que le permitiera realizar una notificación indirecta a través de un mensaje privado en Facebook.

Los perfiles de cada persona incluían la siguiente información:

1.Las fechas de nacimiento de cada uno en Facebook se correspondían con las fechas indicadas en los registros de MKM.
2.Las direcciones de correo electrónico incluidas en Facebook se correspondían con las que el abogado de MKM poseía en sus archivos.
3.La lista de "amigos" de Facebook indicaba que Doña Corbo era amiga de Don Poyser.

Basándose en estas evidencias, el Tribunal aceptó la imposibilidad de realizar una notificación personal, y, puesto que los perfiles de Facebook se correspondían con los de los demandados, el magistrado Harpur ordenó que se notificara la sentencia en rebeldía mediante:

1.Entrega de copia sellada de los documentos relevantes en la última dirección conocida de los demandados.
2.Envío de una copia de los documentos a Don Poyser, a una dirección de correo electrónico determinada.
3.Envío de un mensaje privado a la página de Facebook de los demandados informándoles del fallo y el contenido de la sentencia en rebeldía.

El Tribunal también señaló el hecho de que CSWARE no hubiera mencionado nunca los correos electrónicos hasta después de haber recibido la citación a juicio. Por tanto, el Tribunal de Apelación confirmó la decisión del Tribunal de Primera Instancia.

Fuente: Puede consultarse una traducción y un comentario del caso en inglés por Patrick Van Eecke y Elisabeth Verbrugge en Digital Evidence and Electronic Signature Law Review, 5 (2008) 98 - 102.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

País: China
Citación del caso: República Popular China contra Hong Lei y Sun Xianzhong
Nombre y grado del tribunal: Tribunal Popular del Distrito de Huqiu en Suzhou (provincia de Jiangsu)

Software ilícito · descarga gratuita en China · condena · pena

• SUMARIO

El 20 de agosto de 2009, Hong Lei, propietario del sitio web Tomato Garden (donde la gente puede descargar gratuitamente software pirata, incluido Windows 7) y Sun Xianzhong, su administrador principal, fueron condenados por infracción penal del copyright a una pena de prisión de tres años y seis meses y a una multa de 1 millón de yuanes chinos respectivamente.

El sitio web Tomato Garden se creó en 2003 y se convirtió en un sitio web famoso para descargar software desde el domicilio de los visitantes del mismo. Ahora se trata de un sitio web cerrado. Hong Lei, propietario del sitio web, reprodujo y distribuyó una versión modificada del sistema operativo Windows XP, alterándolo por sí mismo con conocimiento. Esta versión se conoció como la "Tomato Garden Version". El software fue muy descargado y utilizado por los usuarios de ordenadores, debido a que cancelaba el proceso de validación auténtico de Windows XP y cerraba (o desinstalaba) algunas de las funciones de la copia original que no se utilizaban habitualmente. Como resultado de esto, aumentaba enormemente la velocidad del sistema. Además, la descarga del software era gratuita.

En junio de 2008, Microsoft solicitó a la Oficina de la Administración Nacional de Copyright y al Ministerio de la República Popular de China que acusaran al propietario del sitio web. En agosto, se ordenó la custodia policial de Hong Lei en Suzhou, por ser el propietario del sitio web.

Fuente: Jihong Chen, socio del despacho de abogados Zhong Lun (Pekín)

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Editor de la Sección: Stephen Mason

El lector puede enviar detalles de casos o sentencias (tanto civiles como penales) relacionados con la prueba electrónica. En caso de remitir algún caso o sentencia, por favor envíen también la referencia concreta del caso tal y como ésta esté referenciada en su país, juntamente con una copia del mismo o un link a la información.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

• CONFERENCIAS

13 y 14 de octubre de 2009
VII seminario sobre prueba electrónica

Hotel Hesperia, Paseo de la Castellana 57, 28046 Madrid (España)
Objetivo: Cybex y el Consejo General del Poder Judicial han organizado el seminario anual sobre prueba electrónica. Este seminario está dirigido a jueces, fiscales, abogados, miembros de instituciones judiciales y administrativas, y a miembros de departamentos jurídicos, de auditoría, de seguridad y de personal de empresas.

Sitio web: http://www.cybex.es

26 a 28 de octubre de 2009
Conferencia sobre técnica forense aplicada a las tecnologías e investigaciones digitales

National Institute of Standards and Technology (Gaithersburg, Maryland, EE. UU.)
Objetivo: La Conferencia sobre técnica forense aplicada a las tecnologías e investigaciones digitales se basa en los principios de estandarización en el campo de la investigación de la prueba electrónica. Las jornadas abordarán aspectos de muchas de las disciplinas generales de los campos de la investigación de la prueba electrónica para incluir parte de la información más reciente sobre soluciones de software y hardware.

Sitio web: http://www.techsec.com/html/TechnoForensics2009.html

13 de noviembre de 2009
Primer taller internacional sobre minería de datos para la detección de estafas, 2009

Chicago, Estados Unidos
Objetivo: La mayoría de las organizaciones, si no todas, disponen de datos operativos que pueden estudiarse para detectar signos de actividad fraudulenta. Estos datos de las organizaciones generalmente presentan un gran volumen y son heterogéneos, multidimensionales, distribuidos y dinámicos a lo largo del tiempo. En este taller se hará hincapié en las técnicas de minería de datos que pueden aplicarse a los datos de las organizaciones para detectar actividades fraudulentas. La minería de datos se centra en algoritmos para detectar patrones o instancias específicas en datos de alta dimensión de forma precisa. Se trata del primer taller que se centra específicamente en este tema.

Sitio web: https://sites.google.com/site/dmfd09/

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

17 a 20 de noviembre de 2009
DeepSec IDSC 2009

Imperial Riding School, Viena, Austria
Objetivo: DeepSec IDSC es una exhaustiva conferencia europea de dos días de duración sobre seguridad en ordenadores, redes y aplicaciones que se celebra anualmente con el objetivo de reunir en Europa a los principales expertos en seguridad de todo el mundo. Pretende presentar las mejores investigaciones y experiencias de los principales expertos. Está destinada a: responsables de seguridad; profesionales de la seguridad y proveedores de productos; responsables de la toma de decisiones en materia de TI, elaboradores de políticas; administradores de seguridad, redes y cortafuegos; hackers y desarrolladores de software. Los especialistas en prueba electrónica que estén especializados en la ciberdelincuencia pueden encontrar interesante esta conferencia.

Sitio web: https://deepsec.net/

13 y 14 de octubre de 2009
VII seminario sobre prueba electrónica
Hotel Hesperia, Paseo de la Castellana 57, 28046 Madrid (España)
Objetivo: Cybex y el Consejo General del Poder Judicial han organizado el seminario anual sobre prueba electrónica. Este seminario está dirigido a jueces, fiscales, abogados, miembros de instituciones judiciales y administrativas, y a miembros de departamentos jurídicos, de auditoría, de seguridad y de personal de empresas.

Sitio web: http://www.cybex.es

• FORMACIÓN JURÍDICA

14 a 17 de septiembre de 2009
Certificado europeo en la lucha contra la ciberdelincuencia y la prueba electrónica
Chipre
Sitio web: http://www.lexact.com.cy y http://www.cybex.es/ecce/en/

26 a 29 de octubre de 2009
Certificado europeo en la lucha contra la ciberdelincuencia y la prueba electrónica
Italia
Sitio web: http://www.teutas.it y http://www.cybex.es/ecce/en/

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

• FORMACIÓN PARA CUERPOS Y FUERZAS DE SEGURIDAD

7-11 de septiembre de 2009
Programa de formación sobre cibercriminalidad del ISEC - Forensic Scripting using BASH Course (Curso sobre scripting forense con BASH)
Centro de Convenciones Mapfre, Avda. General Perón, 40 - 28020 Madrid, España
Objetivo: este curso formativo forma parte del proyecto de formación sobre cibercriminalidad del ISEC, financiado por el CE. El proyecto paga todos los gastos de viaje, alojamiento y manutención. Todavía quedan plazas para personal de las fuerzas de seguridad de los siguientes países: Bulgaria, la República Checa, Estonia, Finlandia, Grecia, Luxemburgo, Polonia, Eslovaquia, Eslovenia, Suecia, Turquía y la Antigua República Yugoslava de Macedonia. Las personas interesadas en estos cursos se deberán dirigir al Director del Proyectos de Formación, Nigel Jones, en la dirección nigel.jones@ucd.ie, o en el teléfono: +44 7786 317995 si desean más información sobre cómo solicitar una plaza en el curso.

• FORMACIÓN JURÍDICA

26 a 29 de octubre de 2009
Certificado europeo en Cibercriminalidad y prueba electrónica (ECCE)
Italia
Sitio web: http://www.teutas.it y http://www.cybex.es/ecce/en/

• FORMACIÓN PARA PROVEEDORES

Informática forense con EnCase® v6 II
30 de noviembre a 3 de diciembre de 2009
Centro de Convenciones Mapfre, Avda. General Perón 40 - 28020 Madrid (España)
Créditos CPE: 32
Nivel: intermedio
Requisitos previos: Informática forense con EnCase® I No se requiere ninguna formación anterior para este curso.
Objetivo: Este curso práctico se ha elaborado para investigadores con grandes conocimientos de informática, una formación previa en informática forense y experiencia en el uso del programa de informática forense EnCase. El curso se basa en los conocimientos adquiridos durante el curso "Informática forense con EnCase I" y aumenta la capacidad del investigador para trabajar de forma eficaz utilizando las funciones únicas de EnCase.

Sitio web: http://www.cybex.es

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

• RESUMEN SOBRE EVENTOS

El pasado 14 de Septiembre se llevó a cabo el panel titulado: "Privacidad Personal y Profesional (Personal and Professional Privacy)" como parte de las actividades de Eurodig 2009. El panel contó con la participación de distintos expertos de la industria, gobiernos y representantes de organismos europeos, del sector académico y de la sociedad civil.

Entre los aspectos que se trataron y discutieron en el workshop estuvieron:

-privacidad del individuo en el centro de trabajo;
-privacidad en el ámbito de los juegos y mundos virtuales;
-privacidad y protección de datos en redes sociales; y
-estándares globales de privacidad.

El reporte del workshop se encuentra en Español en el blog de Cristos Velasco sobre "Protección de datos y privacidad en México y a nivel internacional" http://www.protecciondedatos.org.mx/?p=111

3 a 4 de septiembre de 2009

Taller sobre institucionalización de la formación de jueces y fiscales en materia de ciberdelincuencia - Proyecto global del Consejo de Europa sobre ciberdelincuencia (fase 2), Estrasburgo (Francia)

Objetivo: En el taller participaron representantes de once instituciones de formación judicial (Alemania, la Antigua República Yugoslava de Macedonia, Bélgica, Croacia, España, Francia, Georgia, Países Bajos, Polonia, el Reino Unido y Rumanía) de la Red Europea de Formación Judicial, además de representantes del sector privado (Microsoft, eBay y Cybex) y académico (UCD) para debatir y acordar un documento de directrices para la formación de jueces y fiscales en materia de ciberdelincuencia y prueba electrónica.

El nuevo concepto consiste en ayudar a las instituciones de formación judicial a llevar a cabo e integrar dicha formación en una formación regular inicial y continua. Además, facilitará la creación de contactos entre jueces y fiscales para mejorar sus conocimientos y promoverá el apoyo sistemático a las iniciativas de formación por los socios interesados.
Sitio web: http://www.coe.int/cybercrime

Editor de la Sección: Stephen Mason

El lector está invitado a enviar información sobre conferencias, cursos universitarios, seminarios legales y seminarios de proveedores directamente al editor de la sección para su inclusión en futuros números del ENAC. Dicha inclusión de eventos y cursos en la sección queda a la completa discreción del editor.

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Editores

Con el fin de editar el "e-Newsletter en la lucha contra el cibercrimen" (ENAC), se ha reunido a un grupo de siete editores, cada uno de ellos experto en la sección del ENAC de la que son responsables.

Los editores se encargan de buscar a los redactores y artículos, y revisar y seleccionar aquellos que consideren más adecuados para incluirlos en el ENAC.

Según el orden de aparición de sus secciones en la ENAC, los editores son:

Sr. PEDRO VERDELHO
Fiscal
pedro.verdelho@gmail.com

Mrs. ESTHER GEORGE
Consejera política Senior y Abogada del Estado
Crown Prosecution Service
Esther.George@cps.gsi.gov.uk

Sra. ELENA DOMÍNGUEZ PECO
Fiscal y Colaboradora de la Agencia Española de Protección de Datos
elena.dominguez@comjib.org

Sr. MATIAS BEVILACQUA
Director Tecnológico
Cybex
mbevilacqua@cybex.es

Sr. NIGEL JONES
Director
Technology Risk Limited
nigel.jones@technologyrisklimited.co.uk

Sra. LILJANA SELINSEK
Profesora adjunta en la Facultad de Derecho de Maribor
liljana.selinsek@uni-mb.si

Sr. STEPHEN MASON
Abogado
Chambers of Stephen Mason
stephenmason@stephenmason.eu

Sra. MIREIA CASANOVAS
Editor Jefe ENAC
Cybex
mcasanovas@cybex.es

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Distribuidores

Para su difusión a nivel mundial el ENAC cuenta con la colaboración de más de 60 Instituciones y Organizaciones que lo distribuirán mensualmente de forma gratuita a los contactos de sus bases de datos.

Si está interesado en ser distribuidor, por favor, póngase en contacto con la coordinadora del proyecto, Mireia Casanovas en mcasanovas@cybex.es.

Los distribuidores del ENAC son, en orden alfabético:

- Actuar Asociación Civil
- Agencia Española de Protección de Datos
- Alba Advisors LTD
- Altmark and Brenna
- Ambassade du Costa Rica
- Asia Pacific Cyberlaw, Cybercrime and Internet Security Institute (Waseda)
- Asociación de Jueces, Justicia y Opinión
- Association of Prosecutors of Republic of Serbia
- Attorney-General's Department Sri Lanka
- Centro de Estudios Judiciários
- CERT-LEXSI
- Ciberdelincuencia.org
- Comisión Interinstitucional Sobre Terrorismo CISTE
- Consejo General de la Abogacía Española
- Conselho Distrital de Lisboa da Ordem dos Advogados

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Distribuidores

Council of Europe

Crown Prosecution Service United Kingdom

Cuerpo Nacional de Policía Española

Cyprus Police Cyber Crime Task Force

Department for International and European Affairs Hungary

Directorate for Investigation of Organized Crime and Terrorism. Prosecutor's Office · High Court of Cassation and Justice

Ebay

Escuela Judicial del Consejo General del Poder Judicial

Espion LTD

Estonian Public Service Academy (EPSA)

EUROJUST

Federal Judicial Police Computer Crime Unit DJF/FCCU Belgium

Federal Judicial Police Brazil

Fiscalía General del Estado Ecuador

Fiscalía General del Estado España

Guardia Civil Española Grupo de Delitos Telemáticos

Home Office United Kingdom

Institute for Arbitration and Mediation

Institute of Criminal Sciences Croatia

Institute of Criminology Faculty of Law · Ljubljana

Institutio Nacional de Tecnologías de la Comunicación INTECO

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Distribuidores

International Training and Methodology Centre for Financial Monitoring

Ledjit Consulting

Lithuanian Bar Association

Malta Police Force

Microsoft

Ministerio della Giustizia Dipartimento per gli Affari di Giustizia

Ministry of Justice and Citizens Liberties Romania

Ministerio Público de Chile Unidad Especializada en Lavado de Dinero, Delitos Económicos y Crimen Organizado

Ministry of Justice of the Slovak Republic

Morenets Consulting

National Institute of Criminology Budapest

National Prosecuting Authority of South Africa

National Public Prosecutor's Office of the Republic of Poland

National School for the Judiciary France

NACPEC.ORG
North American Consumer Project on Electronic Commerce

Organization for Security and Cooperation in Europe

PAD-ORION

Policía Federal Preventive Delegación Coyoacán

Ministerio Público
Procuradoría General de la República Dominicana

RAC
RISK ANALYSIS CONSULTANTS
Risk Analysis Consultants s.r.o. · RAC

SOCA
Serious Organised Crime Agency (SOCA)

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Distribuidores

Sindicatos dos Magistrados do Ministerio Publico Portugal

State Prosecutor Department of Justice Philippines

SUSCERTE
Superintendencia de Servicios de Certificación Electrónica

Technology Risk Limited

Telecommunication Authority Turkey

TEUTAS
TEUTAS srl

The Voivodeship Headquarters of the Police Krakow

unicri
advancing security, serving justice, building peace
United Nations Interregional Crime and Justice Research Institute · UNICRI

University of Buenos Aires

script
University of Edinburgh

University of Maribor

University of Verona

UNODC
United Nations Office on Drugs and Crime
United Nations Office on Drugrs and Crime

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

e-NEWSLETTER EN LA LUCHA CONTRA EL CYBERCRIMEN

El proyecto ENAC está financiado por Cybex y por la Dirección General Justicia, Libertad y Seguridad de la Comisión Europea, en el marco del Programa JPEN Justicia Penal 2008

Aviso legal:

El ENAC ofrece noticias y artículos de opinión como servicio a los lectores. Las declaraciones y opiniones expresadas en estos artículos son únicamente del autor o los autores y pueden no ser compartidas por el equipo de editores del ENAC, la dirección de Cybex o la Comisión Europea.

Las traducciones incluidas en el ENAC han sido preparadas con el mayor de los cuidados. Sin embargo, el equipo de editores del ENAC, la dirección de Cybex o la Comisión Europea no aceptan ninguna responsabilidad sobre la exactitud e integridad de la recopilación y contenido de estas traducciones, o de las consecuencias directas o indirectas de actuar o dejar de hacerlo en base a las mismas.

DL: B.25825-2009
ISSN: 2013-5327

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company