Efectos de los delitos informáticos en el Estado de Veracruz[*]

Dany Elena Hernández García[**]
Carlos Arturo Vega Lebrún[***]

RESUMEN: *El artículo tiene como finalidad analizar a los llamados delitos informáticos, así como hacer referencia del marco jurídico internacional del uso de las tecnologías de la información y sobre todo comparar la realización de estos delitos en legislaciones extranjeras respecto de las pruebas que sirven para acreditar la existencia de tales ilícitos. Considerando la necesidad de la creación de una agencia de investigación especializada, que cuente tanto con equipo de alta tecnología como con una policía cibernética, para que muchas conductas realizadas con el uso indebido de las tecnologías de la información en el Estado de Veracruz, no queden impunes.*

Palabras clave: *delitos informáticos, delitos electrónicos.*

ABSTRACT: *The purpose of this article is to analyze the so-called computer crimes, as well as making a reference of the international legal agenda for the use of technologic information and specially to compare the descriptions of these crimes in foreign law systems and the parameters they have to prove their existence. It is also suggested the need for the creation of a specialized agency, with hi-tech equipment and personnel for a Cyber Police, so the illegal use of technologies may be punished in the State of Veracruz.*

Key words: *computer crime, electronic crime.*

---

[*] Artículo recibido el 10 de enero de 2011 y aceptado para su publicación el 29 de marzo de 2011.

[**] Maestra en Derecho, con especialización en Derecho Penal y Criminología por la Universidad Veracruzana. Servidor Público del Poder Judicial del Estado.

[***] Investigador SNI. Coordinador de CONACyT y Cuerpos Académicos. Coordinación de Investigación del Posgrado. Universidad Popular Autónoma del Estado de Puebla.

Introducción

En la actualidad, el uso de las tecnologías de la información, resulta una herramienta indispensable para el desarrollo de la humanidad, y debido al fenómeno social de la globalización, el cual ha producido un gran impacto en el mundo, en cierta forma ha generado aspectos negativos, puesto que aún cuando la humanidad evoluciona, cierto es que en la misma medida y movimiento social se generan conductas que atentan contra los bienes jurídicos que el estado tutela y respecto del tema en análisis, tenemos a los llamados delitos informáticos, los cuales pueden llevarse a cabo en todo el mundo a través del ciberespacio, desde el punto de vista internacional las legislaciones la mayoría de los países han legislado al respecto, y especialmente en nuestro país los han contemplado en sus legislaciones penales.

En el caso concreto, hablar de dichos delitos en nuestro país, nos conduce a la idea de necesitar conocimientos y habilidades especiales del uso de las tecnologías de la información, al utilizar a la computadora como objetos o instrumentos para llevar a cabo la realización de conductas que pueden vulnerar cuestiones personales, patrimoniales, contra la moral pública, así como ingresar a base de datos, a dañar soportes lógicos o programas informáticos o la información contenida en los mismos; a quienes nos interesa esta problemática, advertimos la falta de uniformidad legislativa (este sería otro tema a tratar en otro artículo), además de percatarnos que nuestras instancias investigadoras, carecen de alta tecnología para poder llevar a cabo un dictamen pericial adecuado para la comprobación de los multicitados delitos, quedando impunes muchos de ellos, lo que se traduce en una vulneración al Estado de Derecho, en el que nos regimos.

En el Estado de Veracruz a partir del año dos mil cuatro, ante la posible serie de conductas ilícitas realizadas a través de las tecnologías de la información, se incorporó en el nuevo Código Penal la figura jurídica de Delitos Informáticos en el artículo 181 del Código Penal vigente en el Estado, sin embargo fue hasta febrero de este año, cuando se radicó una causa penal respecto de éste delito; pero ante la falta de un órgano especializado en conocimientos sobre la utilización y manejo de dichas tecnologías, con las pruebas aportadas en la investigación ministerial, el juzgador no tuvo por acreditados los elementos que componen el delito en análisis.

Lo anterior conlleva a que existen dificultades en la investigación ministerial para recabar las pruebas conducentes y sobre todo su persecución; ocasionando que aquellas personas físicas y morales que se han convertido en sujetos pasivos queden de alguna manera en estado de indefensión, pues hoy en día en Veracruz el tipo penal referido es letra muerta.

Es por ello que el presente artículo tiene por objeto reflexionar sobre la problemática actual que existe en torno a los delitos informáticos y su combate en el Estado de Veracruz, teniendo en consideración las legislaciones internacionales que han empezado a dar solución a este tipo de problemas.

1. Los delitos informáticos, aspectos generales

Para poder entender en que consisten los delitos informáticos, es menester remontarnos al origen de la informática como tal, por lo que sin abundar en el tema, se realizará un breve análisis del origen de la misma.

La informática tiene sus orígenes a finales de la década de los años cincuenta, creada por la Agencia de Proyectos de Investigación Avanzada o por sus siglas en ingles (**ARPA**), perteneciente al Departamento de Defensa de los Estados Unidos, cuyo objetivo era investigar los campos de ciencia y tecnología militar, a través de una red que tuviera la mayor protección de información[1].

Asimismo, a finales de la década de los sesentas, en Inglaterra se generó la primera red con seguridad y protección de información, en el Laboratorio Físico Nacional en Inglaterra, misma que fuera presentada en la ARPA, nombrándola, red ARPANET, la cual funcionaba en un principio con un nodo de información, integrando posteriormente tres más, creados por la Universidad de California en Santa Bárbara, el Instituto de Investigación de Stanford y la Universidad de Utah. Estos sitios (como denominamos a los nodos) constituyeron la red original de cuatro nodos de **ARPANET**, los cuales permitían transferir datos entre ellos, con la finalidad de compartir información.

Para el año de 1971, **ARPANET** había incrementado los nodos, hasta llegar a 15 con 23 ordenadores hosts, los cuales comienzan a utilizar un protocolo de control de redes, creando las primeras interfaces, las cuales eran muy lentas.

En 1972, se realizó la Conferencia Internacional sobre Comunicaciones por Ordenador, en donde se formó un grupo de trabajo internacional para el análisis de protocolos de comunicación que permitirían a ordenadores conectados a la red, comunicarse de una manera transparente a través de la transmisión de paquetes de información, en dicho año se crea un aplicación de correo electrónico que funcionaba en redes distribuidas como **ARPANET**.

Asimismo, fueron la Universidad College London, en Inglaterra y en el Royal Radar Establishment, en Noruega, junto con EE.UU., quienes realizaron las primeras conexiones internacionales, en el año de 1973.

---

[1] CARRETERO, Jesús y otros, *Descubre Internet*, Ed. Pearson Educación-Prentice Hall, Madrid, 2001, p. 17.

En 1974 se estableció el Transmission Control Protocol (TCP), creado por Vinton Cerf y Bob Kahn que luego fue desarrollado hasta convenirse en el Transmission Control Protocol/Internet Protocol (TCP/IP), el cual convierte los mensajes en pequeños paquetes de información, mismos que pueden ser enviados por la red. Asimismo la IP maneja el direccionamiento de los envíos de datos, asegurando que los paquetes de información separados se encaminan por vías separadas a través de diversos nódulos, para 1984 el número de servidores conectados a la red había ya superado los 1.000. Dado que el software de TCP/IP era de dominio público y la tecnología básica de Internet, entendida como la red de comunicación internacional (internacional network) que se maneja mediante los sistemas informáticos[2], la cual permitía conectarse a la red desde múltiples sitios.

En el año de 1986, en los Estados Unidos de Norteamérica, la NSF(por sus siglas National Science Foundation) inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores, permitiendo acelerar el desarrollo tecnológico de internet y brindó a los usuarios mejores infraestructuras de telecomunicaciones.

Ante el desarrollo de la informática, el día 1 de noviembre de 1988 se crea el primer acto que atenta contra las mismas, pues el Internet fue "infectado" con un virus de tipo "gusano". Hasta el 10% de todos los servidores conectados fueron afectados, de ahí que lo que permite observar la ineficacia de los mecanismos de seguridad en Internet.

A partir del ataque a las redes de internet, DARPA decide crear el Computer Emergency Reponse Team (CERT), el cual consiste en un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

Para el año de 1989 el número de servidores conectados a Internet alcanza ya los 100.000. En este mismo año, y para 1992 el número de servidores conectados a INTERNET sobrepasaba la cifra de un millón de servidores, por lo que la ISOC (Internet Society) se formó para promocionar el intercambio global de información.

En ese mismo año se desarrolló la World Wide Web en el Laboratorio de Física en Suiza. Esta tecnología provocó un drástico cambio en la apariencia del internet, generando que para el año de 1993 el número de servidores sobrepasa los 2.000.000, llegando a duplicarse para el siguiente año.

Así, desarrollándose mayores servidores de internet, permitiendo el acceso a la información de manera más rápidas y eficiente, hasta la actualidad, sin embargo, el desarrollo del mismo, trajo aparejado el ataque a los sistemas informáticos y vías de comunicación electrónicas, realizado por los denominados Hackers, consideradas como personas que se dedican a cortar las defensas preestablecidas de los equipos informáticos ajenos o de las páginas web para poder, de esa forma,

[2] http://www.microsoft.com/spain/windows/internet-explorer. Consultado el 15 de octubre del año 2010. Página recomendada por el colaborador Dr. Vega Lebrún.

introducirse y espiar la información ajena o bien producir daños que pueden llegar al borrado total de los datos del equipo al cual se le han cortado las defensas.

Lo anterior ocasiona un serio problema de carácter general, en el cual se comienzan a violar no sólo las comunicaciones privadas, sino también se genera el mal uso de las redes de internet, que lesionan actos y denigran a la sociedad, es por ello que se comienza a construir el esquema de los delitos informáticos en los Estados Unidos de Norteamérica, protegiendo con ello los Derechos Informáticos, considerados como el:

> Conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Sin embargo, no es un término unívoco, pues también se han buscado una serie de términos para el derecho informático como derecho telemático, derecho de las nuevas tecnologías, derecho de la sociedad de la información, iuscibernética, derecho tecnológico, derecho del ciberespacio, derecho de internet, etcétera.[3]

Se consideran delitos electrónicos o informáticos electrónicos**,** a aquellos que son una "especie del género delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en aparatos electrónicos ajenos, y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma especifica la integridad física y lógica de los equipos electrónicos y la intimidad de sus propietarios".[4]

2. El marco jurídico internacional respecto del uso de las tecnologías de la información

En los últimos años y con el desarrollo de la tecnología informática se ha ido perfilando en el ámbito internacional un análisis político-jurídico de los problemas derivados del mal uso que se hace de la misma, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

La primera propuesta de la creación legislativa de protección de los medios informáticos, fue elaborada en 1983, por la Organización de Cooperación y Desarrollo Económico (OCDE), en donde se planteó la idea de aplicar y armonizar en el plano internacional las leyes penales, con la finalidad de luchar contra el problema del uso indebido de los programas computacionales, bajo el argumento de que la delincuencia informática afecta cuestiones económicas de carácter internacional, ante el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información.

---

[3] http://informaticajuridica.com. Consultado el 16 de octubre del año 2010.

[4] CÁMPOLI, G., *Delitos Informáticos en la Legislación Mexicana*, Instituto Nacional de las Ciencias Penales, México, 2005, p. 14.

No fue sino hasta 1986 que la OCDE publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica[5], en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que, los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido, entre otros, asimismo se recomendó que los Estados instituyesen protecciones penales contra otros usos indebidos, espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Por su parte, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "*recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales*".

Asimismo, en la Organización de las Naciones Unidas (ONU), en 1990 durante el desarrollo del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en la Habana, Cuba, se vislumbro el concepto de la delincuencia relacionada con la informática, causada por el mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos, precisando que la mayor injerencia de los delitos informáticos, en ese momento era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, sin embargo, era necesario perfilar un sistema para prevenir nuevos actos ilícitos en materia informática, por lo que se recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Así las cosas, el primer país en legislar en la materia lo fue Estados Unidos de Norteamérica, propuesta llevada al Congreso Federal por el Senador Demócrata Ribicoff[6].

Por otra parte, en la República Mexicana se incluyen los delitos de esta índole el 17 de mayo de 1999, en el Código Penal Federal, con las reformas publicadas en el Diario Oficial de la Federación, dentro de Título Noveno del código punitivo federal, al que se denominó "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática", con lo cual se pretende proteger el acceso no autorizado a sistemas electrónicos o redes informáticas, así como la

[5] LÓPEZ BETANCOURT, Eduardo, *Delitos en Particular*, Ed. Porrúa, México, 2004, p. 270.
[6] *Ibídem* p. 274.

destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia de fondos, dejando libre la facultad de los Estado para plasmar los ilícitos informáticos en sus legislaciones penales.

Asimismo en el año 2004, en nuestro Estado como ya se dijo líneas anteriores, se introdujeron en el nuevo Código Penal los delitos informáticos, justificando los avances que se habían alcanzado con las tecnologías de la información; por lo que desde esa fecha hasta el día de hoy, han transcurrido ya seis años que tiene vigencia dicho código, y sólo en un caso se ha comprobado la existencia del delito informático –que por razones de sigilo no se menciona-, como se ha hecho en otros países, como los son Estados Unidos de Norteamérica por lo que analizaremos tres casos concretos:

CASOS DE DELITOS INFORMÁTICOS				
PAÍS	**DELITO**	**PRUEBAS**	**RECURSOS**	**RESOLUCION**
CASO I MÉXICO (VERACRUZ)	DELITOS INFORMÁTICOS ARTÍCULO 181 FRACCIÓN I CÓDIGO PENAL	DENUNCIA TESTIMONIALES DOCUMENTAL PÚBLICA INFORMES DE LA SHCP	AMPARO	NO SE ACREDITÓ EL CUERPO DEL DELITO
CASO II EE.UU. (NUEVA JERSEY)	FRAUDE INFORMÁTICO	DENUNCIA TESTIMONIAL PERICIAL EN INFORMÁTICA DOCUMENTAL		SE ACREDITA LA EXISTENCIA DEL DELITO
CASO III CHILE	DELITOS DE SABOTAJE INFORMÁTICO			SE ACREDITA LA EXISTENCIA DEL DELITO

Fuente: Cuadro de elaboración propia.[7]

En nuestro país, el caso más concreto sucedió en la ciudad de Perote, perteneciente al Estado Veracruz[8], en donde se interpuso una denuncia por la comisión de delitos informáticos previsto por el artículo 181 fracción I del Código

[7] Fuentes de información, páginas consultadas: http://translate.google.com.mx/translate?hl=es&sl=en&u=http://www.justice.gov/usao/nj/press/files/pdffiles/duro1213rel.pdf&ei=DZLPTPCkAoH7lwe87KzGBg&sa=X&oi=translate&ct=result&resnum=2&ved=0CB8Q7gEwAQ&prev=/search%3Fq%3Dsentence%2Bcase%2BRoger%2BDuronio%26hl%3Des%26biw%3D1280%26bih%3D610%26prmd%3Do. Consultado el 30 de octubre del dos mil diez y http://www.alfa-red.org/enlinea.shtml. Consultado el 18 de octubre del 2010.

[8] Causa Penal del 2010, Distrito Judicial de Jalacingo, Veracruz.

Penal de Veracruz, el cual precisa que "comete delito informático quien, sin derecho y con perjuicio de terceros: I. Ingrese en una base datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información en ellas contenida"; lo anterior bajo el argumento de que el supuesto sujeto activo utilizó de manera indebida la Clave de Identificación Electrónica Confidencial Fortalecida (CIECF), la cual equivale como una firma electrónica, la cual utilizada de manera indebida, suspendió la actividad fiscal de la supuesta víctima del delito, analizando como elementos de prueba la denuncia interpuesta por la agraviada, el acuse de la actividad fiscal del Registro Federal de Contribuyentes, testimoniales, declaración de los inculpados y el informe realizado por la Secretaría de Hacienda y Crédito Público (SHCP), dictando el correspondiente Auto de Formal Prisión, resolución que fuera modificada a través de la resolución del Amparo Indirecto, bajo el argumento de no tener acreditada la figura delictiva prevista por el artículo ya referido, puesto que del material de prueba valorado no se advirtió en ningún momento el ingreso a una base de datos, pues el sujeto denunciado ya tenía la CIECF (Clave de Identificación Electrónica Confidencial Fortalecida) de la agraviada y sólo ingresó al portal de la SHCP, el cual es un portal público y utilizó la misma para suspender su actividad fiscal, por lo que en conclusión no se acredita el delito informático.

De lo anterior se desprende, la carencia en todo momento de la práctica de acopio de medios de prueba del área forense del órgano investigador, para acreditar en los elementos del tipo penal, como lo es el ingreso a una base de datos, quizás por la falta o carencia de los medios eficaces para la comprobación de los mismos, o tal vez la falta de capacitación o información de los encargados de investigar los delitos.

El segundo de los casos, llevado a cabo en la ciudad de Nueva Jersey, EE.UU.[9], donde un exempleado de la compañía UBS Paine Webber, inconformé por el pago de un bono menor a la cantidad esperada, decidió lanzar una "bomba lógica" en un ordenador para que atacará el sistema de red de la compañía, generando perdidas millonarias en la misma y en las máquinas de dicha empresa, las pruebas recabadas durante el proceso, fueron las testimoniales de algunos compañeros de trabajo del inculpado, junto con la denuncia de los apoderados legales de la empresa, sin embargo, las pruebas más importantes fueron recabadas por Agentes del Servicio Secreto de los Estados Unidos de Norteamérica, especializados en materia de crímenes electrónicos, en conjunción con investigadores del servicio secreto de Nueva Jersey, que al realizar la investigación

[9]http://translate.google.com.mx/translate?hl=es&sl=en&u=http://www.justice.gov/usao/nj/press/files/pdffiles/duro1213rel.pdf&ei=DZLPTPCkAoH7lwe87KzGBg&sa=X&oi=translate&ct=result&resnum=2&ved=0CB8Q7gEwAQ&prev=/search%3Fq%3Dsentence%2Bcase%2BRoger%2BDuronio%26hl%3Des%26biw%3D1280%26bih%3D610%26prmd%3Do. Consultado el 30 de octubre del 2010.

a la red de la compañía, pudieron determinar las causas que dieron origen al colapso de la misma, acreditando la culpabilidad del imputado.

Por último, en la ciudad de Chile[10], en los años 2001 y 2002, un empleado de la empresa denominada ATI Chile, al ser despedido, decidió tomar represarías contra la misma, ingresando a los sitios de red de ésta, creando una nueva página de internet en la que se establecieron ofensas para la empresa y argumentando que el sitio web había sido vulnerado, por lo que el administrador de la web al darse cuenta realizó un análisis del sistema de red, percatándose que toda había sido vulnerada; ante tal situación se realizó la querella correspondiente y se recabaron las pruebas necesarias para la acreditación del delito y la búsqueda del inculpado, a través de la brigada del ciber crimen de la policía de investigación de Chile, donde se advirtió que el ataque provenía de un IP de un café internet, y al realizarse el peritaje oportuno en la computadora de dicho lugar, se percataron de que existían programas informáticos que ocasionaron la intromisión a la red, aunado a la confesión del señalado ante la policía, lo que culminó con una sentencia de condena en contra del inculpado; de ahí que se advierta que las pruebas fundamentales fueron las periciales en la materia informática que permitieron precisar el origen del daño y la forma en que se llevó a cabo.

3. La problemática actual para la comprobación de los delitos informáticos en Veracruz

Partiendo del análisis comparativo de los casos anteriormente mencionados, se puede observar que las medidas que se han adoptado a escala internacional para atender esta problemática han avanzado de manera inmediata, sin embargo, cabe precisar que en México y en especial en el Estado de Veracruz, dicho avance es casi nulo, pues la falta de cognoscitiva sobre lo que son los delitos informáticos, la ausencia de una definición jurídica de derechos informáticos, así como la falta de conocimientos técnicos avanzados por parte de los órganos que investigan los delitos ocasiona dificultades de carácter procesal, aunado a la falta de una verdadera armonización de las legislaciones penales para investigaciones nacionales de delitos informáticos, puesto que a nivel federal existe la Policía Cibernética de la Procuraduría General de la República, la cual si bien una de sus funciones es apoyar a las Agencias del Ministerio Público de cada uno de los Estados, para la comprobación de ilícitos llevado a cabo por medio del uso de las tecnologías información, estos casi siempre son en su mayoría para los delitos del orden federal.

[10] http://www.alfa-red.org/enlinea.shtml. Consultado el 18 de octubre del 2010.

Teniendo presente dicha situación, consideramos que la tipificación de los delitos informáticos en Veracruz, resultan ser simbólicos en el Código Penal, pues como ya se enunció sólo existe una causa penal radicada y no se tuvo por acreditada la existencia del delito, esto en razón que para poder dictar un auto de formal prisión debe estar debidamente acreditada la existencia del ilícito, así como la probable responsabilidad penal, y en este caso, las pruebas que integraban la investigación ministerial, no eran aptas para acreditar que los presuntos indiciados habían entrado a una base de datos, siendo de la opinión que ante la falta de una agencia especializada en tecnologías de la información en nuestro Estado, que cuente con una policía cibernética, para que no queden impunes los delitos de esta naturaleza.

Reflexión final

En virtud de lo anterior, estimamos necesario, para resolver los problemas derivados del incremento del mal uso de las tecnologías de la información, es preciso, no sólo desarrollar un régimen jurídico completo, donde se garantice no sólo un bien jurídico tutelado, sino que se abarque todos aquellos que puedan verse afectados con el uso indebido de las tecnologías de la información, como se ha mencionado la creación de una Agencia de Investigación Especializada en tecnologías de la información, que además de contar con equipo de alta tecnología, cuente con una policía cibernética, para así poder alcanzar una verdadera aplicación adecuada del derecho penal vigente, aunado a que consideramos necesario llevar a la Legislatura del Estado una propuesta de reforma respecto de los delitos informáticos en el que se especifiquen los términos referentes a las tecnologías de la información.

Bibliografía

CÁMPOLI, G., *Delitos Informáticos en la Legislación Mexicana*, Instituto Nacional de las Ciencias Penales, México, 2005.

CARRETERO, Jesús y otros, *Descubre Internet*, Pearson Educación-Prentice Hall, Madrid, 2001.

LÓPEZ BETANCOURT, Eduardo, *Delitos en particular*, Porrúa, México, 2004.

Páginas web

http://informaticajuridica.com. Consultado el 16 de octubre del 2010.

http://translate.google.com.mx/translate?hl=es&sl=en&u=http://www.justice.gov/usao/nj/press/files/pdffiles/duro1213rel.pdf&ei=DZLPTPCkAoH7lwe87KzGBg&sa=X&oi=translate&ct=result&resnum=2&ved=0CB8Q7gEwAQ&prev=/search%3Fq%3Dsentence%2Bcase%2BRoger%2BDuronio%26hl%3Des%26biw%3D1280%26bih%3D610%26prmd%3Do. Consultado el 30 de octubre del 2010.

http://www.alfa-red.org/enlinea.shtml. Consultado el 18 de octubre del 2010.

http://www.microsoft.com/spain/windows/internet-explorer Consultado el 15 de octubre del 2010.

Otra fuente

Causa Penal del 2010, Distrito Judicial de Jalacingo, Veracruz.