

## El “phishing” en el Derecho Argentino

### **1.- Introducción:**

La revolución digital supone enormes desafíos para el campo jurídico. Desde hace años, Internet se ha convertido en el medio de comunicación por excelencia, constituyendo una circunstancia que es utilizada tanto con fines lícitos como criminales.

El Derecho, además de adaptarse a los cambios tecnológicos, debe prevenir y sancionar las conductas que, ejecutadas o a través del mundo virtual, afecten negativa y gravemente la convivencia entre las personas.

Los delitos informáticos son *“aquellas conductas disvaliosas socialmente y reprochables desde el punto de vista penal, que concretadas mediante instrumentos y sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquiera de los bienes jurídicos tutelados por la ley, en un momento dado”* (Zarich, Faustina, “Derecho Informático”, Tomo 4, Editorial Juris, Rosario, página 134).

Con mas apego a la teoría penal general, Anzit Guerrero, Tato y Profumo, los definen como: *“toda acción (acción u omisión) culpable realizada por un ser humano, tipificado por la ley, que se realiza en el entorno informático, y esta sancionado con una pena”* (“El Derecho Informático – Aspectos Fundamentales”, ed. Cátedra Jurídica”, pag. 145/6).

En la actualidad, estos ilícitos están legislados por la mayoría de los Códigos Penales modernos, además de que existe una convención internacional sobre el tema, de la que hablaremos más adelante.

Las pérdidas económicas causadas por los virus o las estafas informáticas alcanzan ribetes dramáticos. Salvador Tapia, Director General de Norton Sysmantec para España y Portugal, una de las empresas de antivirus más

grandes del mundo, ha expresado, recientemente, que los cibercriminales mueven, a nivel mundial, un volumen de dinero superior al del narcotráfico y que el 65% de la población ha sido alguna vez víctima en la red, aunque hay quienes desconfían sobre la veracidad de estos datos.

Asimismo, el “medio” a través del cual se consuman los delitos informáticos, permite una gran variedad de posibilidades, que incluyen amenazas, violación a la intimidad, relevación de secretos, prostitución, corrupción de menores, exhibicionismo, etc.

## **2.- Particularidades de los delitos informáticos:**

El modo de comisión de los delitos informáticos les otorga ciertas características que los diferencian instrumentalmente del resto haciendo que su investigación (policial y judicial) resulte mucho más compleja que en otros casos.

En primer lugar, la potencialidad del alcance de las conductas desarrolladas a través de Internet, que no se circunscriben a un ámbito geográfico determinado, sino que pueden esparcirse a través de toda la web, hace que estos crímenes no reconozcan fronteras territoriales. En su mayoría, se trata de delitos transnacionales, como las redes de pedofilia o de lavado de dinero.

En segundo lugar, el anonimato. En muchísimas ocasiones resulta imposible o muy difícil identificar a quién está detrás de una computadora desde dónde se envía un mensaje a través de la red o al responsable de una página web.

Y en tercer lugar, la complejidad técnica del tema y el dinamismo vertiginoso con que evoluciona. El punto más dramático, a mi entender, para la persecución penal de los mismos.

De la combinación de estas características (posibilidades de acceso y alcance casi ilimitadas, anonimato, sofisticación tecnológica y cambios constantes)

se derivan enormes dificultades para que el legislador y la justicia puedan dar una respuesta adecuada a este fenómeno. De ahí, la necesidad de contar con instrumentos de cooperación y coordinación internacionales eficaces que posibiliten llevar a cabo investigaciones rápidas, coordinadas y que permitan la preservación de los elementos de prueba, en procesos cuyas evidencias resultan frágiles y volátiles.

Para este punto, he seguido parcialmente al Dr. Daniel Hargain en “Comercio Electrónico. Análisis jurídico interdisciplinario”, Editorial B de F, Buenos Aires, páginas 22 y 23.

### **3.- Legislación argentina y marcos normativos internacionales:**

El 4 de junio de 2008, con la sanción de la Ley Nº 26.388, se reformó el Código Penal, modificándose ciertos aspectos de los delitos existentes para receptar las nuevas tecnologías. Su texto tipifica como delitos informáticos: la pornografía infantil por Internet u otros medios electrónicos (art. 128, C. Penal); el acceso no autorizado a un sistema o dato informático de acceso restringido (art. 153, bis, C. Penal); la violación de las comunicaciones electrónicas sin la debida autorización, su revelación indebida o la inserción de datos falsos (arts. 155 y 157 bis, C. Penal), el fraude informático (art. 173, C. Penal); el daño o sabotaje informático (arts. 183 y 184, C. Penal) y los delitos contra las comunicaciones (art. 197, C. Penal).

La Ley Nº 26.388 (o la llamada Ley de Delitos informáticos) que se basó en el “Convenio sobre Cibercriminalidad de Budapest” del 23/11/2001, significó un gran avance en la lucha contra la cibercriminalidad.

Esta convención es el primer instrumento legal de carácter internacional sobre la materia, y fue redactada en 2001 por el Consejo de Europa, junto a Sudáfrica, Costa Rica, México, Japón, Canadá y Estados Unidos.

El convenio representa la intención de la Comunidad Europea de unificar su legislación, y de esta forma abordar en forma total y completa el fenómeno de la delincuencia informática.

El Convenio de Budapest sienta los lineamientos básicos en torno a tres áreas fundamentales: la tipificación de los delitos informáticos, los aspectos procesales involucrados en una investigación en torno a estos delitos y las cuestiones relativas a la cooperación internacional, ya que estos ilícitos suelen ser transnacionales. Más de treinta países ya han ratificado esta convención.

Si bien la Argentina, con la Ley de Habeas Data y la N° 26.388, se enmarca dentro de una política nacional sobre delitos informáticos, todavía faltan marcos legales (sustantivos y procesales) eficazmente aptos para recolectar la evidencia en tiempo y forma, necesitando en muchas ocasiones de la acción coordinada entre la policía y los magistrados de otras naciones.

#### **4.- La estafa informática en la legislación argentina**

La figura de la estafa informática se encuentra consagrada en el inciso 16 del art. 173 del Código Penal, al disponer que: *“El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos”*.

La disposición agregada al art. 173 del Cód. Penal clausuró la discusión doctrinaria y jurisprudencial acerca de si el concepto de fraude era aplicable a la manipulación informática, por aquello de que el sistema informático no podía ser engañado ya que seguía procesos preestablecidos. Siendo así, quizás hubiera sido sistemáticamente mas apropiado ampliar al efecto, la descripción del art. 172 del Cód. Penal.

Sostiene Pablo A. Palazzi en “Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388”, Editorial Abeledo Perrot, año 2009, que la acción típica es defraudar mediante una manipulación en un ordenador.

Indica el autor que el tipo penal no se refiere solamente a procesos informáticos que son modificados, sino a *“cualquier supuesto de defraudación mediante ordenadores, como accesos ilegítimos mediante claves falsas o phishing o falsos montajes en cajeros automáticos... Es una suerte de tipo penal abierto en relación con cualquier abuso informático”*.

Pallazi señala, ateniéndose al texto de la norma, que la *“manipulación informática” debe alterar el funcionamiento del sistema informático o la transmisión de datos. No se trata de cualquier manipulación, sino de aquella que es apta para producir dicho efecto. Si por un error en la programación, no se logra alterar el sistema informático, estaremos ante un delito tentado o imposible*”. Uno de esos procedimientos es el conocido en el mundo informático como “phishing”.

Esta nueva modalidad de defraudación, desde que se inserta en la enumeración del art. 173 del Cód. Penal, requiere que exista un perjuicio patrimonial y ello se debe producir mediante la disposición o la afectación patrimonial, en la cual el medio específico es la manipulación informática o la transmisión de datos.

## **5.-El “phishing” - Concepto:**

El término “phishing” –así se conoce en el ambiente informático- proviene de la palabra inglesa “fishing” (pesca) y alude al intento de hacer que los usuarios “piquen en el anzuelo”. Para su explicación, transcribiré la definición publicada por Microsoft en Internet, la cual si bien es larga, resulta didáctica a los fines de este trabajo:

*“El phishing es una modalidad de estafa diseñada con la finalidad de robar (y aprovechar económicamente, le agrego) la identidad ajena. El delito consiste en obtener información... como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños... el usuario malintencionado envía millones de mensajes falsos que parecen provenir*

*de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos.*

*La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales. Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial.*

*Estas copias se denominan sitios Web piratas. Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad”.*

Cabe señalar que existen otras modalidades de “phishing”, cuyo análisis supera el objetivo de esta exposición.

## **6.- El phishing en la jurisprudencia argentina**

El 3 de agosto pasado, en los autos caratulados “G.R. y otro s/ procesamientos, Expte. N° 39.779”, la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional confirmó el procesamiento de dos personas imputadas por fraude, a raíz del uso de la técnica de manipulación informática conocida como “phishing”.

Se les imputa a los acusados haber llevado a cabo maniobras de fraude, mediante la creación de una página paralela, por la cual obtuvieron los datos necesarios (código de transferencia y número de tarjeta de crédito) para poder operar en las cuentas bancarias de la víctima y el 9 de septiembre de 2009

efectuar dos transferencias de 780 y 770 pesos desde la caja de ahorro y cuenta corriente de ésta a otra caja de ahorro, todas de la misma entidad bancaria.

Es decir que los imputados, a través de un sitio paralelo, obtuvieron datos de dos cuentas bancarias, desde las que transfirieron dinero, sin el consentimiento del titular de esas cuentas.

El denunciante manifestó que el 8 de septiembre pasado, mientras verificaba el estado de su cuenta bancaria, en su computadora, vía Internet, apareció una pantalla paralela que le indicaba que ingresara su código de transferencia y número de tarjeta de débito, lo que hizo debido a que ello daría una mejor atención y seguridad en la operación.

Al día siguiente, la víctima advirtió que faltaba dinero de su cuenta corriente y de su caja de ahorro, el cual había ingresado en una tercera cuenta, del mismo banco y cuya titularidad fue aportada por esa entidad, identificando así a los presuntos estafadores.

En ese contexto, señaló el tribunal que la circunstancia de que el dinero de la víctima haya ingresado en la cuenta de uno de los procesados, al día siguiente de la obtención de los datos, mediante la manipulación informática (página paralela) denunciada es suficiente como para agravar la situación procesal de los indagados

La Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional estableció que el hecho de que no se haya determinado de qué computadora se realizaron las transferencias, no altera de momento los graves indicios cargosos, y más si se tiene en cuenta que uno de los procesados es perito mercantil con orientación en computación.

La conducta reprochable fue encuadrada dentro de las previsiones del art. 173, inciso 16, incorporado al Código Penal mediante la Ley N° 26.388 y que castiga con pena de un mes a seis años, a quien “*defraudare a otro mediante*

*cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos”.*

### **7.- Valoración del fallo “G.R. y otro s/ procesamientos, Expte. N° 39.779”**

En este caso, la víctima habría sido desapoderada del dinero depositado en sus dos cuentas bancarias, mediante la obtención de sus datos confidenciales a través de un ardid informático, siendo posible identificar a los supuestos autores del ilícito a través del seguimiento financiero de los fondos sustraídos: datos que fueron proporcionados por la misma entidad financiera.

En relación al fallo, el Dr. Ricardo Sáenz, Fiscal General ante la Cámara Criminal y Correccional de la Capital Federal y especialista en delincuencia informática, en su página web [ricardosaenz.com.ar](http://ricardosaenz.com.ar), manifestó que “...no encontraremos en esta decisión judicial un análisis acabado de este delito, y ello no se debe a un defecto del fallo sino a que se ha dictado en un momento embrionario de la investigación, anterior al juicio...”.

Continua diciendo, el Dr. Sáenz, que la propia resolución de los jueces reconoce que todavía no se han probado todos los pasos del procedimiento del phishing, ni se ha determinado de qué computadora se realizó la transferencia. Sin embargo, considera como determinante para confirmar el procesamiento que el dinero ingresó en la cuenta de los imputados al día siguiente de la obtención de los datos, “mediante la manipulación informática (página paralela) denunciada” por la víctima, y que aquéllos no pudieron dar una explicación satisfactoria sobre el origen del depósito en su cuenta. Estas reflexiones confirman el aserto sobre la dificultad técnica que afrontan estas investigaciones, ya que si bien el ingreso de la transferencia en la cuenta de los imputados configura un indicio grave no llega a la condición de no contingente, ya que no podría descartarse absolutamente la existencia de una maniobra de algún tercero para afectar a los procesados o con otros fines. El cine, que a veces se adelanta premonitoriamente, ya se ha ocupado de esta

especulación (v. “Red de Mentiras”, Título Original: Body Of Lies, USA, Año: 2008).

La importancia de este precedente radica, básicamente, en tratar una realidad que en nuestra jurisprudencia se encontraba relegada o poco considerada, esperando que abra un camino en donde los operadores jurídicos le otorguen la atención que el tema se merece en el futuro próximo o inmediato.

## **8.- Conclusiones:**

El uso de los sistemas informáticos abre nuevas formas de ataque a los bienes jurídicos protegidos, como la propiedad, la intimidad y la libre comunicación, y de ahí la acuciante necesidad de que los Estados repriman estos ataques con efectividad y eficiencia.

Si bien la Argentina ha dado pasos certeros en la lucha contra el ciberdelito, es imprescindible, para ganar la batalla, contar con un marco legal e institucional apropiado a las exigencias y complejidades de este flagelo criminal y, por tanto, con funcionarios policiales y judiciales altamente capacitados para intervenir en la investigación de estos ilícitos y con la disposición de los instrumentos materiales adecuados para identificar a sus autores y partícipes como para seleccionar, recoger y asegurar la evidencia.

Hoy en día, dependemos absolutamente del acceso y del buen funcionamiento de una computadora para realizar cualquier actividad diaria. Internet, las computadoras y los sistemas informáticos son herramientas imprescindibles para el desarrollo humano.

Y como sostiene acertadamente Pablo Palazzi, en su obra “Delitos informáticos”, Ad-Hoc, 1° edición, Buenos Aires, 2000, p. 45: *“La interdependencia de las máquinas hará que el ataque a las mismas constituya un delito que supere la lesión al bien individual para afectar un bien colectivo. Es aquí donde entran los*

*delitos contra la seguridad pública, las telecomunicaciones y los medios de transporte”.*

Y justamente el Derecho tiene como misión regular esta nueva realidad (la de las “nuevas tecnologías”), la cual ha modificado radicalmente la forma de vida de toda la humanidad. -

Este artículo de opinión pertenece al sitio web MilaWEB (<http://www.milaweb.com/blog/>). Se agradece que en caso de ser citado o transcrito, se respete la fuente original.