LOS DELITOS INFORMATICOS EN LA ERA DE LA REVOLUCIÓN CIENTÍFICO-TECNOLÓGICA: HACKING, CRACKING, PHREAKING, PHISHING, SCAMMING.

Prof. Dr. Ramiro Anzit Guerrero.

La revolución científico-tecnológica. La revolución informática y sus consecuencias sobre el hombre y la sociedad. La Sociedad de la Información.

Los avances tecnológicos generan grandes cambios en las actividades humanas, tanto en el orden privado como el público, aunque especialmente en aquellas de contenido económico. Estos cambios implican en muchas ocasiones nuevos intereses susceptibles de entrar en conflicto y plantear situaciones que no pueden ser abordadas adecuadamente por las normas preexistentes.

A modo de ejemplo, en las postrimerías del siglo XIX la aparición de la fotografía instantánea y el avance de la tecnología que permitió multiplicar las ediciones de los medios masivos de comunicación, trajeron como consecuencia la difusión con una amplitud hasta el momento desconocida de hechos y eventos, los cuales afectaban la intimidad de las personas, llevando a que la doctrina y luego la jurisprudencia tuvieran que forzosamente redefinir el concepto de “intimidad”. Del mismo modo, la invención del automóvil a comienzos del siglo XX trajo nuevos elementos y problemáticas que debieron ser abordados por varias ramas del Derecho; como los accidentes de tránsito en sus aspectos civiles y penales, y la modalidad de venta por concesionarias o por círculos cerrados en sus aspectos civiles, penales y comerciales.

Los avances científicos y tecnológicos han venido modificando con aceleración constante la forma de vida de las sociedades, determinando que a mediados del

siglo XX la llamada “Sociedad Industrial” fuera reemplazada por la llamada actualmente “Sociedad de la Información”.

La “Sociedad de la Información” se caracteriza fundamentalmente en que la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas, convirtiéndose sin lugar a dudas en bienes intangibles altamente valorados. La “Sociedad de la Información” surge a partir del desarrollo científico-tecnológico, en una relación dialéctica de mutua alimentación: el desarrollo científico-tecnológico hace nacer la sociedad de la información, la cual potencia el desarrollo tecnológico, lo cual a su vez acelera el avance de la sociedad de la información.

Entre los primeros teóricos que consideraron la aplicación de computadoras a la actividad jurídica podemos mencionar Lee Loevinger, jurista norteamericano, quien en 1949 acuñó el término “jurimetría” para referirse al uso de computadoras en el derecho. Más adelante, Hans Baade formaliza la jurimetría como disciplina 1963, al editar la obra “Jurimetrics: the Methodology of Legal Inquiry”.

La primera aplicación de una máquina de cálculo al ambiente jurídico se realizó en la Cámara de Representante del estado de Ohio (EE.UU.) en el año 1938, al comenzar a utilizarse una máquina de tarjetas perforadas para el control y seguimiento de las iniciativas de ley presentadas.

A partir de los años cincuenta se desarrollan las primeras investigaciones para la búsqueda y recuperación de documentos jurídicos en forma automatizada; pasando de utilizar las computadoras sólo para tareas matemáticas a utilizarlas con elementos lingüísticos. Fue en la Universidad de Pittsburg, Pennsylvania, a través del Health Law Center, donde el director llamado John Horty concibió la idea de crear un mecanismo a través del cual se pudiera tener acceso a la información legal de manera automatizada.

Para el año 1959, el mencionado centro de la Universidad de Pennsylvania colocó los ordenamientos jurídicos de Pennsylvania en cintas magnéticas, convirtiéndolo en el Estado que da nacimiento a la recopilación legal Informática. En 1960, en Washington D.C., se realiza ante la Asociación Americana de Abogados la primera demostración del sistema. Posteriormente la Corporación de Sistemas Aspen

rediseñó el mencionado sistema legal y comenzó a explotarlo comercialmente. Fue de esta forma como la automatización de los ordenamientos legales de ese país fue ganando espacios. En 1966, doce estados de los Estados Unidos tenían este sistema y para 1.968, cincuenta estados de ese mismo país lo acogieron.

Puede considerarse como otro logro para el desarrollo de la Informática Jurídica, el sistema Lite (Legal Transformation Through Electronics), también desarrollado por el Health Law Center antes mencionado, y hoy llamado Flite (Federal Legal Transformation Through Electronics) que posibilita la búsqueda de información en miles de fallos de la Corte Suprema a través de computadoras. Este sistema fue originariamente desarrollado bajo contrato con la Fuerza Aérea Norteamericana en el año 1969; y actualmente contiene 7.407 fallos de la Corte Suprema entre 1937 y 1975, contabilizando un total de 14,5 millones de palabras.

En la década de los sesenta se comienzan a desarrollar varios sistemas de informática jurídica. En 1964 la Corporación Americana de Recuperación de Datos comenzó a explotar comercialmente sistemas de procesamientos de datos legislativos. En 1967 aproximadamente, la Corporación de Investigación Automatizada de la Barra de Ohio, desarrolló sistemas enfocados hacia los abogados litigantes, llamado sistema OBAR. Sin embargo, los trabajos referidos a este sistema fueron continuados en 1970 por Mead Data Central, que comenzó a explotarlo comercialmente en 1973 bajo el nombre de sistema LEXIS.

Paralelamente IBM comenzó a desarrollar investigaciones en al área de recuperación de documentos. A partir de esos desarrollos se crea el sistema de procesamientos de documentos de IBM, llamado IBM- TEXTPAC, que comenzó a utilizarse en. Otro sistema desarrollado fue el STAIRS, utilizado por varios estados de Estados Unidos.

Delitos Informáticos

Concepto

Para la teoría penal general, los elementos integrantes del delito son:

- El delito es un acto humano consistente en una acción u omisión.
- Dicho acto humano ha de ser antijurídico, es decir, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe ser un acto típico, es decir, debe corresponder a un tipo legal definido por ley.
- El acto ha de ser culpable, es decir, imputable a dolo (intención) o a culpa (negligencia). Una acción es imputable cuando puede ponerse a cargo de una determinada persona
- La ejecución u omisión del acto debe estar sancionada por una pena.

Resumiendo lo antedicho, un delito es: una acción típica, antijurídica y culpable realizada por un ser humano, y sancionado por una pena.

Aplicando el concepto de delito al Derecho Informático, se define al delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, tipificada por La Ley, que se realiza en el entorno informático o mediante el elementos informáticos, y está sancionado con una pena.

Debemos destacar en la anterior definición que el elemento informático puede intervenir como medio o como objeto. Interviene como medio cuando se utilizan elementos informáticos para realizar la acción delictiva. Por ejemplo, utilizar una computadora para falsificar dinero. Interviene como objeto cuando la acción delictiva tiene como fin el daño a un sistema informático. Por ejemplo, cuando un virus borra información de una computadora.

Clases

Los delitos informáticos, en cuanto a sus clases, se clasifican según seas delitos contra la propiedad (dentro de los cuales el hurto, la estafa, el daño y la usurpación de la propiedad intelectual), delitos contra la intimidad (como la

violación del correo electrónico), o delitos contra la seguridad pública y las comunicaciones (generalmente como agravante del delito de daño).

Las Organización de las Naciones Unidas (ONU) reconoce diferentes clases de delitos informáticos. Son categorizados de la siguiente manera:

A. Fraudes cometidos mediante la manipulación de computadoras

   Este tipo de delito consiste en manipular los datos de entrada, los programas que procesan los datos, o los datos de salida.

   A.1 Manipulación de datos de entrada: es el modo más sencillo de fraude informático, debido a que no requiere conocimientos informáticos especiales. A modo de ejemplo, podemos mencionar la inclusión de una solicitud de gastos adicional en un lote, o el aumento de un monto de gasto.

   A.2 Manipulación de programas: este delito consiste en modificar un programa o insertar nuevos elementos; para que el programa realice funciones para los cuales no fue creado; perjudicando a un tercero. Por ejemplo, la inclusión de personas ficticias en una nómina de pago, para lo cual se modifica el programa de administración de nómina salarial con el fin de que esos datos ficticios no aparezcan en los reportes.

   A.3 Manipulación de datos de salida: se considera que el fraude es por manipulación de los datos de salida cuando el mismo se efectúa realizando acciones con el fin de alterar el resultado de una operación. El ejemplo más común es la falsificación de tarjetas de crédito, cuyo fin es alterar los datos de salida del cajero automático, lo que implica que entregará dinero.

   A.4 Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una o más cuentas, para ser transferidas a otra u otras. Se basa en el principio de que 10,66 es igual a 10,65 pasando 1 centavo a la cuenta del ladrón un número importante de veces de modo tal

que, al cabo de un tiempo, resulte en una cifra significativa. Esta técnica también puede aprovechar los decimales de redondeo en al cálculo de los porcentajes sobre servicios que presta el banco (comisiones).

B. Falsificaciones

B.1. Como objeto: se produce cuando se alteran documentos almacenados en una computadora.

B.2 Como medio: se produce cuando se utiliza una computadora para realizar una falsificación.

C. Daño: se realiza a través de diferentes modalidades

C.1 Virus: Son programas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema informático por medio un programa legítimo que ha quedado infectado; o a través de puertas abiertas por otros programas conocidos como “Caballo de Troya” o “Troyano”. Una vez activados, pueden operar en el sistema provocando diferentes problemas, como el borrado de archivos o la inhabilitación de componentes, entre otros.

C.2 Gusanos: Se crea del mismo modo que un virus, con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Sin embargo, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

C.3 Bombas Lógicas y Cronológicas: Son programas que destruyen la información en un sistema informático, a partir de un evento denominado “disparador”. En las bombas lógicas, el disparador es un evento determinado, por ejemplo, el escribir cierta secuencia alfanumérica, o el ejecutar cierta cantidad de veces un programa. En las bombas cronológicas, el disparador es el paso del tiempo. Han existido diversos casos muy publicitados de bombas que se activaron en determinada fecha.

D. Acceso no autorizado a servicios y sistemas informáticos (hacking)
   Es el acceso no autorizado a sistemas informáticos por motivos diversos, desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
E. Piratas informáticos o hackers: El acceso se efectúa a menudo desde un lugar exterior, recurriendo diversos medios. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
F. Reproducción no autorizada de programas informáticos de protección Legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos, algunos países, entre ellos la República Argentina, ya han tipificado como delito esta clase de actividad, sometiéndola por ende a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna, especialmente los sistemas denominados P2P (peer to peer).

En la República Argentina, tanto la reproducción no autorizada de programas informáticos, como el acceso no autorizado a sistemas informáticos y el fraude o daño producido a sistemas informáticos, se encuentran tipificados penalmente a partir de Junio de 2008, con la sanción de la ley 26.388. Además de Argentina, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España y Chile han emitido su legislación en materia de delitos informáticos.

La ONU considera que el problema de los delitos informáticos se eleva a la escena internacional, por cuanto éstos constituyen una nueva forma de crimen

transnacional y su combate requiere de una eficaz cooperación internacional concertada. La misma ONU aporta un análisis de los problemas que rodean a la cooperación internacional en el área de los delitos informáticos, cuyos puntos más destacados son:

- Ausencia de acuerdos globales en relación al tipo de conductas deben constituir delitos informáticos.
- Falta de acuerdos globales en la tipificación de dichas conductas delictivas.
- La transnacionalidad de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de una cooperación internacional efectiva.

Delitos informáticos como medio y como objeto: Hacking, Cracking, Phreaking, Phishing, Scamming

El término "hacking" (del inglés “to hack”, que traducimos como “cortar”, “hacer tajos”) refiere a la técnica consistente en acceder a un sistema informático sin autorización. Existe autorización cuando el sistema está conectado a una red pública y no dispone de un control de acceso mediante el uso de identificadores de usuario y passwords. El hacking se produce tanto cuando se accede sin autorización a un sistema informático, como cuando se accede a funcionalidades o información por sobre el nivel de autorización concedido. Por lo general, el hacker no tiene intención de causar un daño, sino que su motivación radica en el desafío de violar sistemas de seguridad. Aunque también existen motivaciones comerciales a partir de las cuales se han producido eventos de hacking con el fin de obtener información de, por ejemplo, tarjetas de crédito.

Existe también la actividad conocida como “ethical hacking”, que se realiza a pedido y bajo contrato, con el fin de poner a prueba las medidas de seguridad de un sistema informático.

El cracking consiste en la creación de programas o rutinas que permiten inutilizar los sistemas de protección establecidos por el titular de los derechos de propiedad intelectual sobre una aplicación informática. El término viene del inglés “to crack”, que significa “romper”. Dentro de las numerosos tipos de “cracks” existentes, se destacan los que permiten seguir utilizando un programa de demostración una vez superado el periodo de prueba establecido. También existen cracks que eliminan la llamada del programa a una llave electrónica, disco llave o número de serie; o generan aleatoriamente números de serie para un programa determinado.

En el concepto "phreaking" (la palabra deriva de la conjunción de “phone” –teléfono- y “cracking”) se engloban las técnicas de fraude en materia de telefonía analógica y digital. Uno de los métodos más utilizados en antiguamente fue el de las denominadas "cajas de colores", que emitían distintas frecuencias, en función del resultado perseguido. Por ejemplo, las cajas azules utilizaban la frecuencia de 2600 hercios empleada por los operadores telefónicos para efectuar llamadas sin cargo. En la actualidad, el phreaking está relacionado principalmente con la manipulación de telefonía celular, como por ejemplo la actividad de “desbloquear” un teléfono, que implica permitir que ese teléfono sea utilizado en cualquier red de telefonía celular (y no sólo en la red de la compañía que vende el dispositivo); o la actividad de modificar el código IMEI, que identifica unívocamente el equipo celular, actividad que está muy vinculada al robo de aparatos celulares.

El phishing (en español, “pesca”) consiste en el envío de correos electrónicos a una persona con información falsa, con el fin de que esta persona envíe datos personales al remitente. Un caso muy común consiste en el envío de un correo electrónico simulando ser un banco, donde se solicita al usuario que ingrese a un sitio para validar cierta información bancaria (como por ejemplo una transferencia de dinero o algún problema con la cuenta). El sitio al que es enviada la persona cuando hace clic en el hipervínculo del correo electrónico, también es falso, pero con la apariencia de ser el verdadero sitio del banco, con el fin de que la persona ingrese su clave bancaria. Una vez ingresada la clave, el falso sitio bancario emite un mensaje de error, o re direcciona al usuario al verdadero sitio del banco son que este lo note. Bajo esta metodología, pueden obtenerse fácilmente muchas

claves de usuarios, ya sean bancarias, de tarjetas de crédito, de correo electrónico, de acceso a empresas, o cualquier otra clave de tipo personal. En Enero de 2004, la FTC (Federal Trade Commission) en los Estados Unidos llevó a juicio el primer caso contra un "Phisher" sospechoso. Un joven de California que creo una página Web que aparentaba ser de la empresa America Online para poder robar números de tarjetas de crédito. El 1º de marzo del 2005, también en los Estados Unidos, el senador Patrick Leahy introdujo el Acta Anti-Phishing. Esta ley federal establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de e-mail con el afán de embaucar a los usuarios podrían recibir una multa de hasta 250.000 dólares y penas de cárcel por un periodo de hasta 5 años.

El scamming (del inglés "scam", que significa "estafa") se realizan a través de correos electrónicos con el fin de obtener dinero de la víctima. Dentro de los más conocidos, se encuentra la "Escenario de Estafa de Viaje", donde un supuesto servicio de pareja ofrece contactos con mujeres de Europa del Este, los cuales comienzan en el sitio y pasan rápidamente a ser por contacto directo con la mujer deseada por correo electrónico, para más adelante continuar por teléfono (ella dice que no tiene teléfono, así que utilizarán un servicio de voz por Internet, o ella lo llamará a él). Finalmente, la mujer solicita 1.000 o 2.000 euros para viajar al país de la víctima. Estas estafas pueden durar varias semanas, o meses, desde el primer contacto hasta el pedido del dinero, estableciendo el marco psicológico de credibilidad en la víctima. Una variante de la misma estafa es la llamada "Escenario de Estafa de Accidente", que consiste en, luego de varios meses de relación "virtual", inventar un accidente automovilístico en la familia por el cual requiere que le envíe dinero para la operación. Otros "scamming" tradicionales son los correos electrónicos que felicitan a la víctima por haber "ganado" un premio de lotería, de algún concurso, o una "green card". En estos casos, la víctima deberá pagar alguna tasa de transferencia de dinero, o proveer información de identidad y cuentas bancarias o tarjeta de crédito. Algunas otras estafas están relacionadas con supuestas herencias que la víctima ha recibido en el exterior, o la propuesta para realizar una operación económica con un gobierno africano corrupto. Otra

recurrente forma de engaño es la de recibir una gran cantidad de millones de dólares (que no pueden ser sacadas de cierto país por diferentes motivos). La oferta requiere que la víctima transfiera a su propia cuenta el dinero a cambio de un porcentaje de comisión. A este método se lo llama “The Nigeria Advance Fee Scam” o “Four-one-Nine”. Estos engaños, también llamados Cartas Nigerianas, son uno de los casos de “Scam” más utilizados. En ellas el remitente dice ser familiar o tener algún tipo de relación con una persona que ha fallecido y ha dejado una importante suma de dinero en un banco, que por algún motivo no puede sacarlo del país, y necesita transferirlo a la cuenta de otro particular. El destinatario de este mail, sería recompensado con un porcentaje de esta transacción. En el caso de que el destinatario responda el correo, el estafador enviara una serie de documentos que aparenten corroborar la historia, y una vez lograda su confianza, le pide al usuario una suma de dinero para costear abogados y algún tipo de documentos para realizar la operación. En todos los casos, el “scammer” apunta a despertar las bajas pasiones de la víctima, a través del dinero o el sexo, y así subyugar el impulso racional que lo llevaría a dudar de la situación.

Sin configurar un delito, existen los “Hoax”, que son correos electrónicos de contenido falso, distribuidos en cadenas, que tienen por objeto difundirse en la red. Generalmente, su contenido importa noticias sobre acontecimientos alarmantes, personas perdidas, personas que necesitan ayuda por un trasplante, o la promesa de un “premio” de una empresa informática por vez que ese correo sea enviado. Estos correos electrónicos incluyen la solicitud de ser reenviado a los contactos de la persona que lo ha recibido. La finalidad de los “hoax” puede ser simplemente distribuirse, o pueden ser utilizados para obtener direcciones de correo electrónico válidas, debido a que las direcciones de destino generalmente aparecen en el cuerpo del correo electrónico al ser reenviados. De este modo, se pueden crear bases de datos con correos electrónicos válidos, muy útiles y valiosas para el marketing. Algunos “hoax” que han circulado por Internet han sido: “Falsa alerta de infección que copia ventana de NOD32”, “Alerta sobre falsa actualización de Microsoft”, “Troyano disfrazado de reproductor de Macromedia Flash”, “Troyano

simula ser actualización de antivirus", "Agua en botella de plástico produce cáncer", "La noche de las dos lunas, sobre la noche en que Marte ser vería tan grande como la Luna".

Ley 26.388

El 4 de Junio de 2008, por 172 votos a favor y 0 en contra, fue sancionada la Ley 26.388 de Delitos Informáticos, incorporándose así Argentina a la lista de países que cuentan con regulación legal sobre esta importante cuestión.

La Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal (C.P.) con figuras propias y específicas, sino que es una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del C.P. actualmente en vigencia, con el objeto de regular las conductas que emergen a partir de las nuevas tecnologías, como medios de comisión de delitos previstos en el C.P.

La reforma contempla el perfeccionamiento de la comprensión de términos como "documento" y "firma" que fueron ampliados a los conceptos digitales de los mismos. Otro aspecto destacado de la modificación establecida por la Ley 26.388 es que otorga a los correos electrónicos, y a cualquier comunicación electrónica (por ejemplo, los mensajes de texto enviados por celular, o el tráfico de información por Internet) la misma protección que tienen la correspondencia epistolar y de telecomunicaciones (art 153. C.P.); plasmando definitivamente en la normativa la tendencia jurisprudencial al respecto. Es importante destacar que la violación o desvío de comunicación electrónica debe ser realizado "indebidamente" de acuerdo al tipo legal. La inclusión del término "indebidamente" obedece a que no le queden dudas al intérprete respecto a requerir la finalidad dolosa del autor del delito, y evitar cualquier razonamiento tendiente a considerar comprendidos en el tipo a quienes, en procura de mejorar el servicio que prestan a sus usuarios, activan mecanismos de protección, tales como antivirus, filtros o algoritmos de desvío de correo electrónico para evitar el ya mencionado SPAM.

A lo largo de su articulado también tipifica, entre otros, los siguientes delitos informáticos:

A. La pornografía infantil por Internet u otros medios electrónicos (art. 128 CP), penando al que estuviere relacionado con la producción de pornografía con menores de 18 años, con su distribución; y al que facilitare pornografía a menores de 14 años.
B. El acceso a un sistema o dato informático (artículo 153 bis CP), penando la conducta conocida como "hacking", es decir, a quien accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido; con un agravante cuando el delito fuera cometido contra una institución estatal, o una institución privada que preste un servicio público o un servicio financiero.
C. En su art. 155, el C.P. amplía la protección de la intimidad a las comunicaciones electrónicas, penando la publicación de las mismas sin la debida autorización. Concordantemente, el art. 157bis del C.P. pena el acceso indebido a bases de datos; o revelare indebidamente información registrada en una base de datos; así como también pena a quien insertare datos falsos.
D. El art. 173 C.P. tipifica el fraude mediante la manipulación de sistemas informáticos, dando por finalizada la discusión doctrinaria y jurisprudencial acerca de si el tipo delictivo "fraude" era pasible de ser aplicado al fraude a computadoras, debido a que el sujeto pasivo en ese caso (el sistema informático) no era pasible de ser "engañado"; sino que inevitablemente seguía procesos preestablecidos.
E. Asimismo, los artículos 183 y 184, incisos 5º y 6º C.P. tipifican el daño o sabotaje informático, penando a quien alterase, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. Este tipo penal zanja otra discusión doctrinaria y jurisprudencia existente hasta ese momento, acerca de si era posible provocar "daños" a bienes intangibles como los programas

de computación, los cuales no estaban enmarcados dentro de la categoría de “cosas”, por no ser materiales.

F. El art. 197 del Código Penal tipifica los delitos contra las comunicaciones.