Carlos Tablante

Delitos informáticos

delincuentes sin rostro

Una propuesta legal para enfrentar las amenazas del ciberespacio

Prólogo: Carlos Genatios

En cambio

Carlos Tablante nació en Maracay, el 29 de octubre de 1954. Inicia su carrera política muy joven, militando en el MAS desde el nacimiento de esta organización política. Se desempeñó como concejal en el Distrito Ricaurte y Diputado a la Asamblea Legislativa de Aragua (1979-84). Diputado al Congreso de la República (1984-89). Fue primer vicepresidente de la Cámara de Diputados. Participó en la Comisión Especial que redactó la Ley Antidrogas (Losep) y fue miembro de la Comisión Parlamentaria redactora del Proyecto de Ley contra el Crimen Organizado. A mediados de los años 80 publicó el libro *El sindicato del crimen*. En 1989 se convirtió en el primer Gobernador del Estado Aragua electo por el voto popular, responsabilidad que ejerce durante seis años, al ser ratificado por el pueblo. Actuó como Ministro Antidrogas de Venezuela. Es creador de la Fundación Encambio. Participó en la redacción de la Constitución de la República Bolivariana de Venezuela, como miembro de la Asamblea Nacional Constituyente. Actualmente es Diputado a la Asamblea Nacional.

DELITOS INFORMATICOS, DELICUENTES SIN ROSTRO

Delitos informáticos, delincuentes sin rostro

Una propuesta legal para enfrentar las amenazas del ciberespacio

CARLOS TABLANTE

En Cambio
Espacio para la Utopía Posible

Primera edición
Caracas, 2001

Edición a cargo de
LoCreativo Comunicación

Coordinador de edición
William Castillo Bollé

Equipo de investigación
Pilar Suárez Sasso
Vivian Jiménez

Diseño gráfico
Comala.com

Diseño portada
LoCreativo Comunicación

Impresión
Fanarte

Impreso en Venezuela

INDICE

PRÓLOGO

El vertiginoso incremento de Internet en Venezuela

A partir del año 1999, Venezuela ha registrado un significativo incremento del número de usuarios de Internet. Actualmente una población de aproximadamente 5% de los venezolanos tiene acceso a este servicio. Datanálisis reporta un crecimiento del 300% de usuarios de Internet entre el año 1999 y el segundo semestre del año 2000. Por otra parte, Júpiter Communications, empresa de referencia en esta área, señala que Venezuela tendrá una población estimada de 3,8 millones de usuarios para el año 2005. Estas cifras colocan a Venezuela como el país con el crecimiento más acelerado en el uso de Internet en América Latina, con una proporción de 1.167% entre el año 1999 y el año 2005. El segundo país es México con un 877% de crecimiento en ese mismo lapso de tiempo, y a continuación siguen Colombia y Argentina con una proporción del 780% en cinco años. Por otra parte, el crecimiento del comercio electrónico en América Latina también señala a Venezuela como el país con las tasas más aceleradas de desarrollo en este renglón económico.

Para el año 1999, Venezuela contaba con transacciones en el orden de cuatro millones de dólares y se estima que para el año 2005 (de acuerdo a las cifras de Júpiter Communications), Venezuela realizará operaciones comerciales por unos 350 millones de dólares. Esto representa la tasa de crecimiento más alta de América Latina, con un valor de 8.600% seguida por Argentina con un crecimiento de 7.193% y México con 6.060%. Estos desarrollos que se han dado en Venezuela de manera tan significativa, reflejan también el violento crecimiento de Internet en nuestro país. Para el año 1981, la red de redes a nivel

mundial sólo contaba con 213 huéspedes, y en enero del año 2000 ese número se elevó a 72 millones. A manera de ejemplificar también este importante crecimiento, solamente el día 27 de marzo de ese año se crearon 3.6 millones de páginas. Actualmente los motores de búsqueda sólo cubren un 15% de la red.

En un mundo de 6.000 millones de habitantes, solamente 275 millones están conectados a Internet, de los cuales la mitad de la población corresponde a los Estados Unidos y Canadá. En nuestros países la brecha tecnológica es tal, que podemos señalar que en Venezuela el 60% de la población nunca tocó un computador. Dentro de este contexto difícil, pero al mismo tiempo halagador, dado el importante crecimiento de Internet en nuestro país, debemos señalar cuáles han sido las políticas de Gobierno, que han permitido este vertiginoso posicionamiento de Venezuela en el uso de la red de redes. El crecimiento de estas tecnologías obedece a la implementación de cinco ejes fundamentales de acción: Capacitación, Desarrollo de Contenidos, Desarrollo de la Conectividad, Economía Digital y Gobierno Electrónico.

El primer elemento, la Capacitación, representa el mayor reto para nuestros países, porque tenemos la finalidad de mejorar las condiciones de vida de nuestra gente y de impulsar el desarrollo económico en la región más desigual del planeta, Latinoamérica. La capacitación para el uso de Internet en Venezuela ha sido objeto de políticas agresivas que comienzan a implementarse desde el Ministerio de Educación y el Ministerio de Ciencia y Tecnología, impulsando la atención a la población de manera libre y continua a través de un intenso programa de creación de 240 Infocentros a nivel nacional de acceso gratuito a Internet. Así mismo, han sido desarrollados y están en proceso de implementación distintos programas para la creación de centros de informática en las Escuelas Bolivarianas y diversas escuelas del país, así como el impulso de la utilización de Internet en los Institutos Universitarios Tecnológicos y la creación de carreras en el área de Tecnologías de Información y Comunicaciones a nivel universitario y a nivel de postgrados. También deben ser incluidos los esfuerzos para

crear redes a nivel internacional que fortalezcan los centros de generación de conocimiento en Venezuela en el área de software y de tecnologías de información, tomando en cuenta las importantes capacidades que existen actualmente en el país y vinculándolas de manera muy estrecha con los centros de excelencia a nivel mundial. Esto ha permitido orientar también políticas de cooperación de postgrado tanto a nivel nacional, como a nivel internacional. Dentro de este aspecto de la Capacitación también deben resaltarse los esfuerzos realizados desde el Ministerio de Ciencia y Tecnología para acercar los programas de estudio de los distintos países de la región latinoamericana y generar de esa manera contenidos que puedan ser compatibles.

El segundo punto, el Desarrollo de Contenidos en Internet, es otro de los elementos fundamentales que se han impulsado desde el Ministerio de Ciencia y Tecnología con la finalidad de contribuir significativamente al desarrollo de Internet en Venezuela. En tal sentido, en la actualidad se están implementando programas en las áreas de salud, educación y producción y comercio. En el área de educación, el Ministerio de Educación ha establecido los lineamientos fundamentales que especifican los contenidos que deben ser desarrollados en multimedia e Internet, lo que ha permitido realizar convocatorias públicas a los empresarios y a las universidades para el desarrollo de los mismos, siguiendo las líneas y exigencias de la educación venezolana. Por otra parte, el Ministerio de Ciencia y Tecnología, las Universidades Nacionales y algunas empresas privadas que han trabajado conjuntamente con Alcaldías y Gobernaciones a nivel nacional, están impulsando programas en el área de Telemedicina, con la finalidad de llevar los beneficios de Internet a la población del país, mejorando la prestación de servicios.

La tercera línea de acción es la Conectividad, ésta es atendida mediante la implementación de los lineamientos definidos en la Ley de Telecomunicaciones. Esta Ley, promulgada el 12 de junio del año 2000, abre el espacio para el desarrollo de las telecomunicaciones impulsando la búsqueda del acceso universal y de la prestación de servicios de calidad y de diversidad para todos en el país. Así mismo,

contempla la creación de un fondo de investigación en el área de Telecomunicaciones, el cual está siendo formado con la finalidad de atender necesidades fundamentales de investigación en las áreas que permitan fortalecer nuestras capacidades para el desarrollo de las telecomunicaciones.

Como cuarta línea de acción tenemos el desarrollo del Gobierno Electrónico. Para ello, fue creado desde el Ministerio de Ciencia y Tecnología, el Centro Nacional de Tecnologías de Información, en marzo del año 2000 y en mayo de ese mismo año fue dictado el Decreto 825, que establece a Internet como prioridad nacional. Este Decreto exige la creación de estrategias de desarrollo y modernización en cada uno de los ministerios, con la finalidad de mejorar sus capacidades administrativas y la prestación de servicios a los ciudadanos. Ha quedado demostrado a nivel internacional, que Internet permite agilizar los trámites administrativos, así como incentivar la participación de los ciudadanos en la toma de decisiones y supervisión de la gestión pública, profundizando de esta manera la participación democrática, mejorando la prestación de los servicios y luchando significativamente contra la corrupción.

En algunos países se ha logrado utilizar Internet para llevar adelante consultas públicas y dentro de este marco podemos citar, por ejemplo, la ciudad de Porto Alegre, donde se hacen consultas a las comunidades sobre la mejor manera de implementar el presupuesto de la Alcaldía de la ciudad. Así mismo, en Villa del Salvador, en el Perú, se realizan consultas a nivel comunitario sobre decisiones fundamentales que deben ser tomadas en las Alcaldías mediante el uso de Internet.

Como quinta línea de acción tenemos la economía digital, la cual, como señalamos en un comienzo, ha tenido un importante crecimiento en el país. En tal sentido, en el pasado mes de febrero de este año 2001 fue promulgada la Ley de Firmas y Documentos Electrónicos, creada por el Ministerio de Ciencia y Tecnología con una activa participación del sector académico, gubernamental y empresarial, y permite actualmente establecer un sustrato mediante el cual se

reconoce el contenido de los documentos que sean utilizados por vía electrónica. Esto era un elemento fundamental para la certificación electrónica y el desarrollo de la economía digital en Venezuela. La publicación de la Ley corresponde a la Gaceta Oficial 37.148 y su promulgación se hizo a través de la Ley Habilitante, en el Decreto Ley 1.204 del 10 de Febrero del año 2001. El objetivo de esta Ley es el de otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, así como regular lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.

La Ley presenta entre sus características más resaltantes, que otorga valor probatorio a los mensajes de datos y firmas electrónicas de manera idéntica a los instrumentos escritos. La Ley no se inclina en particular por alguna tecnología específica, sino que contempla todas las tecnologías existentes y las tecnologías por venir, por lo tanto, se puede decir que es una Ley neutra desde el punto de vista tecnológico. En esta Ley se especifica claramente que la utilización de la firma electrónica es voluntaria y no sustituye a la firma manuscrita. Tampoco altera las formas de los actos jurídicos registrales y notariales existentes. Por otro lado, otorga reconocimiento jurídico a los mensajes de datos, las firmas electrónicas y los servicios de certificación.

Dentro de la Ley se crea una Superintendencia de Servicios de Certificación Electrónica, como servicio autónomo dependiente del Ministerio de Ciencia y Tecnología, con el objeto de acreditar, supervisar y controlar a los proveedores de servicios de Certificación, tanto públicos como privados. Dentro de las expectativas que se crean con esta ley se considera que los impactos deberán incrementar la inversión extranjera en recursos humanos calificados y en nuevos servicios, productos y tecnologías. Así mismo, se espera ahorrar en compras, en servicios de telecomunicaciones, y en compras y licitaciones del Estado, así como disminuir el tiempo estimado de procesamiento de información intra y entre entidades públicas, incrementar el número de usuarios de Internet, y crear y reforzar empresas en el sector, generando nuevos productos y servicios en tecnologías de información.

Una vez promulgada la Ley de Firmas y Documentos Electrónicos el paso siguiente corresponde al establecimiento de mecanismos que permitan luchar contra el delito cibernético. En tal sentido, en Venezuela contamos en estos momentos con dos propuestas que avanzan en esa dirección, una de ellas es la presentada por el Diputado a la Asamblea Nacional, Carlos Tablante, cuyo título es *Ley contra Delitos Informáticos*, cuya propuesta está contenida en el presente libro. Esta propuesta sienta las bases para el inicio de un profundo debate a nivel nacional sobre un tema tan importante como el que nos hemos referido actualmente.

Carlos Genatios
Ministro de Ciencia y Tecnología

Nota del autor

El presente libro nació a partir del trabajo de investigación encomendado a la Subcomisión de Fraudes Informáticos de la Asamblea Nacional de Venezuela. Dado el elevado número de denuncias que recibimos en la Asamblea Nacional, relacionadas con la clonación de tarjetas de crédito y débito y otros fraudes electrónicos vinculados al sector financiero, la Comisión de Finanzas de dicho cuerpo decidió en septiembre del año pasado abrir una investigación al respecto, creando esta Subcomisión, cuya jefatura nos fue encomendada.

Gracias al aporte de un valioso grupo de venezolanos, abogados, académicos, expertos, gerentes de instituciones financieras, funcionarios públicos, policías, periodistas e investigadores –entre otros– fue surgiendo la necesidad de proponer una Ley Especial que atendiese ya no sólo el fenómeno del fraude digital sino que, como Ley Penal, abarcara el conjunto de modalidades delictivas que se efectúan a través de los medios teleinformáticos.

La razón de esta decisión es simple y apremiante. Los delitos informáticos no se reducen sólo al fraude vinculado con la banca electrónica, como la clonación de tarjetas o el *hacking* de cuentas bancarias, sino que abarca un amplio espacio de peligros: representan una enorme pérdida de divisas para los autores de *software* y otros productos por culpa de la piratería, para citar un caso. La piratería devora un vasto porcentaje del mercado de video juegos, de programas, de CD's y videos, porque estos piratas no pagan derechos de autor y ponen en jaque la propiedad intelectual.

Pero hay otros peligros aun más aterradores en el ciberespacio, delitos que usan la teleinformática para globalizarse sin fronteras: la delincuencia organizada –narcotráfico, trata de blancas, tráfico de

armas, lavado de dinero– el terrorismo, la propaganda extremista, la pedofilia, y hasta la presencia de información que podría ser utilizada eventualmente para la fabricación de armas de destrucción masiva, químicas o nucleares.

A lo largo de la investigación, en la medida en que fuimos comprendiendo la complejidad del fenómeno y constatamos el nivel de desinformación presente en la sociedad venezolana, sentimos el deber de elevar el grado de información y concientización entre los actores públicos, privados y ciudadanos respecto a las novedosas y peligrosas formas que adopta el delito digital, también llamado delito informático o ciberdelito.

Por todo lo anterior, consideramos la presente propuesta como un paso adelante en la dirección correcta, en tanto la Asamblea Nacional, en cumplimiento del mandato emanado de la Constitución de la República Bolivariana de Venezuela, realiza la necesaria y urgente reforma del Código Penal Venezolano.

Así, en medio de numerosas consultas, fue moldeándose la idea de este libro, cuya finalidad no es sólo presentar una Ley que, a fin de cuentas, deberá someterse al examen de los legisladores, sino también llamar la atención pública sobre este delicado tema.

Es fundamental que el Estado venezolano aborde el problema de los delitos informáticos como un asunto de políticas públicas, vinculado a la seguridad del Estado, que requiere medidas estratégicas, porque se trata de un fenómeno que va más allá de la simple manipulación de medios electrónicos y tiene que ver con el delito organizado y con la propia inserción de los medios digitales en nuestra sociedad.

Es por esa razón que en este texto, sin ánimo de invadir el terreno de los expertos en informática, hemos realizado un esfuerzo por brindar una visión amplia que permita entender los efectos que el fenómeno digital, y en particular el de la delincuencia informática, están ejerciendo y ejercerán en los próximos años en nuestra sociedad.

La revolución informática y digital está vinculada con un fenómeno al que hemos prestado atención anteriormente: el de la globalización. Hemos dicho que la globalización tiene dos caras: por un

lado hay ventajas evidentes, pues se trata de procesos, tecnologías y herramientas que nos pueden ayudar a luchar contra la pobreza, las enfermedades, el hambre, la exclusión y la marginalidad.

Pero por otra parte, hasta ahora sólo se globalizan las tecnologías y los flujos de capitales, pero no las políticas sociales, no la lucha contra la pobreza y a favor de la solidaridad. Para nosotros la revolución informática es una fuente novedosa e inagotable de conocimiento y educación, que no puede dedicarse sólo a la producción de dinero, como si fuera una ruleta de divisas, sino que puede servir para profundizar la democracia, en tanto proporciona nuevos espacios para el debate, pues son millones los foros y debates que se realizan en tiempo real y en todo el mundo sobre temas de política, ecología y muchos otros.

Pero estas potencialidades sólo pueden realizarse en la medida en que haya acceso real a las herramientas de la informática para todos los ciudadanos.

Los delitos informáticos son otra parte negativa de la globalización. Y como hemos dicho, la globalización está allí para que la usemos, para que saquemos de ella beneficios para nuestros pueblos, y para que la controlemos en sus peligros.

Con este aporte queremos contribuir entonces a ofrecer herramientas para controlar los peligros de la globalización, y para darle el sentido humano que nos corresponde exigir en tanto dirigentes políticos comprometidos con la ideología de la solidaridad.

Muchas personas e instituciones han contribuido de forma consistente y valiosa a la realización de este trabajo. En primer lugar, quiero dar las gracias a la Dra. Beatriz Di Totto, brillante abogada y docente, y a la Dra. Magaly González, quienes armaron la estructura legal del proyecto. Al Dr. Gregorio Quiñones, quien es un pionero en la investigación penal de estos delitos en nuestro país. Al Dr. Bayardo Ramírez Monagas, redactor de la LOSEP y del Proyecto de Ley Contra la Delincuencia Organizada y su influencia corrupta. Al Dr. Jorge Luciani, autor de importantes libros sobre la prevención contra el lavado de dinero. También a los Dres. Fernando Fernández y Fernando

Rodríguez, quienes apoyaron con sus criterios y juicios la orientación de esta investigación. A William Castillo Bollé, quien coordinó el proyecto editorial. A Pilar Suárez Saso, que aportó sus conocimientos en el área de lavado de capitales, a Vivian Jiménez, investigadora, y a mi esposa Margarita, bajo cuya dirección hemos desarrollado toda el área de publicaciones de la Fundación EnCambio.

En nombre de la Subcomisión de Fraudes Informáticos de la Asamblea Nacional, de los diputados que la integraron, Norberto Peña, Guillermo Palacios, Elías Mata, Héctor Vargas, y de la Fundación EnCambio, queremos agradecer a todas las instituciones públicas y privadas que, con sus visiones y análisis, enriquecieron esta investigación y esta propuesta.

Carlos Tablante

Materia y poder: de los átomos a los bits

Entre las obsesiones vitales de la sociedad occidental, lo material ocupa sin duda un lugar predominante. Dominar, transformar y aprovechar la materia que se encuentra en la naturaleza, explotarla y exprimirla al máximo, ha sido históricamente una de las claves del sistema capitalista. No en balde hemos sido bautizados como una sociedad materialista, sistema basado en la adoración a lo material, en una confianza ciega en la apropiación, transformación y aprovechamiento de los bienes naturales en todas sus manifestaciones, mediante la ciencia, la técnica y el trabajo.

En cierta forma, la historia del capitalismo moderno desde el Renacimiento para acá puede escribirse como la historia de una afanosa y violenta búsqueda de fuentes de materia prima en todo el mundo y su posterior conversión en productos para el consumo masivo, bajo reglas de fabricación y mercadeo a gran escala. Fe que la Revolución Industrial no hizo más que amplificar a través de las máquinas y la tecnología.

Pero el mismo desarrollo tecnológico, la aparición de la electricidad y con ella de los medios de comunicación de masas entre finales del siglo XIX principios del XX, trajeron a escena a una nueva materia prima: la información. A diferencia del carbón o del petróleo, esta nueva materia prima no se podía ni medir ni contar de la misma manera. Se trataba, en principio, de la reproducción de la realidad (imágenes, voz, datos) y seguidamente de su multiplicación rápida, de su difusión masiva, de su comunicación a través de grandes distancias.

Con la invención de la imprenta Gutenberg ya había prefigurado el rol que la información tendría sobre la sociedad al hacer accesible las sagradas escrituras, y también su crítica, a miles de personas. Los

nuevos medios (el telégrafo, el cable submarino, la fotografía, el cine, la radio, el teléfono y la televisión), abrirían a la información una dimensión insospechada. Se creó una nueva cultura, la cultura de masas, surgida de la difusión masiva de mensajes e información. Se ampliaron los públicos y los mercados. Se multiplicaron por mil las posibilidades del comercio. Millones de seres humanos pudieron acceder a bienes culturales, antes propiedad de las élites. Se aceleró el proceso industrial de producción. La información se convirtió definitivamente en poder, porque el poder empezó a definirse como el control de las mentes y no sólo como control de los territorios y los yacimientos.

A medida que la tecnología para producir y transmitir información se hacía más sofisticada (sistemas satelitales, sistemas de información aeronáutica, computadoras) y la información se expandía más y más, el poder comenzó a desplazarse lentamente de las minas a los centros de producción tecnológica, del campo a la oficina, de las fábricas a los medios de comunicación. Ahora, además del acceso a las materias primas, y el dominio de los mercados y los ejércitos, era necesario también controlar la producción y los medios de información.

En los últimos años, la rápida evolución de las tecnologías de la información, la unión entre el desarrollo informático y las telecomunicaciones, entre computadoras y redes de comunicación, bautizada como teleinformática ha abierto paso a lo que algunos llaman la sociedad informatizada o sociedad de la información. Un conjunto de fenómenos sociales y económicos como la liberalización de los mercados, la extensión de la libre competencia, la creciente división del trabajo y la necesidad de una mayor racionalización en el uso de los recursos naturales, fenómenos que forman parte del proceso de globalización, ha estimulado una creciente demanda de servicios de comunicación rápidos y a bajo costo que están cambiando el rostro del planeta y de los modelos sociales.

Es un hecho que el sector de las tecnologías de la información, conocidas en la literatura como IT (information technology), ha pasado a convertirse en uno de los motores de la economía mundial. En algunas de las naciones desarrolladas ya más de la mitad de la población activa

se ocupa del manejo de información. Tres de cada cuatro nuevos empleos se genera en el sector de la teleinformación, y en más del 55% de los hogares en dichas naciones existe, además de la televisión, un computador personal.

Hablamos hoy de una sociedad de la información, porque ésta no sólo es masiva en términos de grandes emisiones o de transmisiones vía satélite desde los grandes centros a sus periferias, sino en la medida en que la teleinformática ha hecho accesible la incorporación de los ciudadanos a las redes de comunicación y sirve para que éstos se hablen, se formen y se informen, intercambien bienes y servicios, se diviertan, se eduquen sin fronteras y sin reglas.

La cara más visible de este fenómeno es sin duda Internet, la llamada red global o autopista de la Información. Su veloz transformación desde un proyecto de alcances militares hasta una poderosa tecnología de comunicación mundial, que crece en algunos lugares del mundo a una tasa superior al 10% mensual y llega ya a más de 250 millones de personas en todo el mundo, ha empezado a transformar profundamente la cultura, la economía y el funcionamiento de la sociedad.

Bill Gates ha definido este fenómeno como el advenimiento de una nueva etapa histórica para la humanidad, tal como fueron la Edad del Bronce o la Edad de Piedra: vivimos, dice, el nacimiento de la Edad de la Información. Para Nicholas Negroponte[1], uno de los más respetados gurús en la materia, los átomos están siendo reemplazados por los bits[2] o unidades de información, como la pieza clave del sistema económico y cultural. *Estamos atravesando la transición de una sociedad basada en el dominio de la materia prima a una sociedad orientada en el dominio, generación y uso de la información.*

Otros autores son menos optimistas y ven en este proceso el definitivo del triunfo de la economía y el capital transnacional

---

1 Nicholas Negroponte. *Being digital.*

2 Unidad mínima de información, corresponde en el lenguaje binario mediante el cual funcionan las computadoras a una instrucción (1/0 - SI/NO - ON/OFF - Blanco/Negro).

globalizado, que impone ahora su ley en el mundo mediante el uso de las redes y las computadoras, destruyendo la diversidad cultural, creando nuevas y más profundas formas de estratificación y discriminación social entre los ciudadanos, y entre las naciones ricas altamente informatizadas y los países pobres. Para estos críticos, la brecha digital, la diferencia entre quienes pueden acceder y usar las redes digitales y los que no, amenaza con hacer más profunda e irreversible la brecha económica y social.

Pero, sea cual sea la postura que asumamos, la verdad es que hoy en día todo el debate social y económico pasa necesariamente por valorar y considerar el efecto que la teleinformación, las tecnologías de la información y los fenómenos digitales están ejerciendo sobre la vida privada y pública, la economía, la cultura, el conocimiento y el ambiente. Este debate es ineludible y requiere de la sociedad y del Estado una respuesta a la altura de la velocidad y complejidad de los procesos.

CLICS A LA SOCIEDAD DE LA INFORMACIÓN

¿Cómo funciona la nueva sociedad de la información?

La teleinformación básicamente es una herramienta tecnológica y social que permite a una persona, utilizando las redes de telecomunicaciones, acceder e interactuar con información almacenada en bancos de datos remotos mediante el uso de computadores. Hay quienes ven en la teleinformática un nuevo medio que ayudará a los humanos a resolver problemas organizacionales, educativos y económicos hasta absorber tareas rutinarias y devolvernos más tiempo libre para el ocio productivo. Hay otros que la ven como una amenaza a la privacidad, a la seguridad de los datos, y al mismo intercambio libre de información mediante el control tecnológico que puede ejercer poderes supraterritoriales.

Lo que no se discute hoy día es que la información digital, en la

multitud de formas en que está disponible, telefonía, datos, imágenes, video, software, está modificando múltiples aspectos de la actividad humana. Se trata de un proceso profundamente social y humano, no meramente tecnológico. A fin de cuentas, los computadores reciben, almacenan, procesan y despliegan información. A través de las redes mundiales esta información viaja o circula entre las personas y las máquinas que las interconectan. Ciertamente, los computadores pueden manipular la información a una mayor velocidad que las personas, pero a diferencia de éstas, las máquinas no «entienden» la información que manipulan, en su cerebro o «chip» la información es simplemente una secuencia de símbolos binarios, una serie de instrucciones en unos y ceros regida por impulsos eléctricos. Esto significa, después de todo, que la sociedad de la información es aún un asunto entre humanos, diseñada y manejada por seres con virtudes y defectos.

Por ello, el término sociedad de la información alude a un proceso histórico de transformación de modelos sociales, económicos y culturales y no puede ser encerrado entre los muros de la tecnología. Los hábitos, la cultura, la forma de comunicarnos, de intercambiar bienes y servicios, está siendo alterada y este cambio es de una dimensión tan excepcional que sobrepasa todo lo anteriormente conocido.

¿Qué es el ciberespacio?

Es un término algo difuso en su definición. Para algunos, el ciberespacio se reduce a Internet, la red mundial más difundida y de mayor acceso, un espacio virtual donde la gente habla por medio de servicios de conversación o chats, transmite datos mediante el correo electrónico (*e-mail*), compra y realiza transacciones de todo tipo, accede a información, maneja y crea nueva información. Para otros, como William Gibson[3], quizás el primero en mencionar el término, es una invención imaginaria: allí detrás de las pantallas de las computadoras existe un sitio tan profundo que no puede verse todo de una vez, pero

3 En su famoso texto *Neuromancer*.

que sabemos que está allí porque podemos sumergirnos y navegar en él para manejar información. Resulta curioso que el término ciberespacio sugiera algo tan vasto y desconocido como lo era el mar durante la Edad Media, de allí que el término «navegar» signifique viajar dentro de este espacio insondable y «navegadores», sean los programas o naves virtuales que nos conducen a través de éste.

¿Qué son las redes?

Las redes son los canales, los puentes, los túneles que interconectan a personas, computadoras y dispositivos de telecomunicaciones local, regional y globalmente. A veces las redes son vistas como las carreteras o autopistas de la información, o como el asfalto de éstas, donde viaja la información que se intercambia y se crea en el ciberespacio. Se expresan a veces de forma virtual, como Internet, popularizada como «La Red» , o pueden existir físicamente mediante cables, fibra óptica, modems, satélites, señales y antenas de radio.

A través de las redes se hacen negocios, investigación, educación, cultura y vida social. Investigaciones apologéticas afirman que de los dos mil usuarios de Internet conectados en 1983 (prácticamente todos en Estados Unidos) el número de conectados a las redes teleinformáticas alcanzará la extraordinaria cifra de mil 800 millones en el 2002, y que antes del año 2012 podría igualar al número de habitantes del planeta. Aunque tal vez un tanto exageradas, la realidad es que para comienzos de este año, sólo por Internet, la red o autopista más grande y popular, viajaban ya más de 250 millones de usuarios. Ningún otro fenómeno en la historia de la humanidad ha tenido un crecimiento tan explosivo.

El fenómeno de las redes se expande al ritmo del impulso de las nuevas tecnologías de la información. Redes locales y regionales se están interconectando cada vez más con Internet para así volverse nodos o puntos de entrada de una vasta red global. En Chile, por ejemplo, un ambicioso proyecto denominado Enlaces, usando Internet, ha estado conectando a todas las escuelas del sector público desde

hace varios años, permitiendo crear una sola comunidad virtual de todos los estudiantes del equivalente de la Escuela Básica. Es una red dentro de la red que une a estudiantes, docentes, padres y Estado en un mismo espacio de educación, conocimiento y colaboración.

Pero las redes son también un ambiente social, un sitio o una forma de encontrarse con otras personas, una intersección de sistemas teleinformáticos con sistemas sociales. Como sucedió con el teléfono, la radio y la televisión, la gente adopta los nuevos medios de comunicación y cambia su forma de vida para adaptarse. Hoy muchos jóvenes viven «pegados a la red» y manifiestan lo que el crítico Hakim Bey llama «cibergnosis», una suerte de seudo religión de internautas fanáticos de las redes, que creen haber encontrado un espacio de vida autónomo, donde supuestamente crean una nueva cultura (la cibercultura) o cultura alternativa al mundo real. En la práctica, los servidores, modems y redes de comunicación suministran la infraestructura tecnológica de la comunicación mediante la conexión de computadores[4], mientras las personas van adaptando sus conocimientos, agregando contenido y creando nuevas rutinas para su uso. De hecho, hoy hablamos de la Generación Net[5], como aquella generación que ha nacido ya en un ambiente completamente computarizado y cuya habilidad para moverse en el entorno informático proviene de un aprendizaje natural.

¿Qué es Internet? (De la Guerra Fría a la Red Global)

En 1962, en pleno auge de la Guerra Fría entre los bloques comunista y capitalista, la instalación de una batería de misiles nucleares en Cuba por parte de la Unión Soviética generó un pánico colectivo en los Estados Unidos. Ante la eventualidad de un ataque nuclear lanzado a 90 millas de su territorio, el Gobierno norteamericano ordenó al

---

4 Académicamente este fenómeno es denominado también CMC: Computer Mediated Comunication. Comunicación mediante Computadores.

5 La generación de la red, o nacida en la red.

Pentágono el desarrollo de un sistema de comunicación, de una red, entre los principales centros y bases militares alrededor del mundo, que fuese capaz de sobrevivir a un ataque con armas nucleares. La idea era crear una «red inteligente», que pudiese seguir conectando los centros de mando aunque algunos puntos (o nodos[6]) de la red fueran puestos fuera de combate.

La clave de este proyecto era que la información debía ser lo suficientemente sagaz para descomponerse, viajar a través de diferentes sistemas (satélites, cables submarinos, líneas telefónicas), escogiendo las mejores vías, y ser capaz de reconstruirse en el punto de llegada. Sólo así se podía garantizar la interconexión, la seguridad de los datos y secretos militares, y por ende la permanencia del poder militar norteamericano ante la eventualidad de un conflicto nuclear a gran escala.

El proyecto, idea de la administración Kennedy, fue encargado al Departamento de Investigaciones Avanzadas del Pentagóno (ARPA). Años después, entre 1968-69, la red Arpanet, como fue bautizado el proyecto, estuvo concluido en su estructura básica. Los protocolos o lenguajes informáticos creados por los científicos militares, permitían cumplir el objetivo encomendado. Por su filosofía, por la manera en que fue diseñada, Arpanet era una red indestructible. Los datos e informaciones militares, secretos de Estado y de investigación, podían viajar dispersos en pequeños paquetes inteligentes de información mediante computadores que «hablaban» un mismo lenguaje o conjunto de códigos llamados TCP-IP[7]. Gracias a la amenaza de la Guerra Fría, y a la unión entre tecnología, telecomunicacciones y poder militar, había nacido el embrión de lo que años más tarde sería conocido como la red de redes, Internet, o las autopistas de la información.

No hubo, afortunadamente, guerra nuclear, y a principios de los 70, la poderosa Arpanet fue transferida a la no menos poderosa Fundación Nacional de la Ciencia de los Estados Unidos (National Science Foundation-NSF) para su investigación y desarrollo. La

---

6 Nodo: punto de conexión a una red.
7 TCP: Transfer Control Protocol. Protocolo de Control de Transferencia. IP: Internet Protocol. Protocol de Internet.

red militar fue rebautizada como NSFNET, una red que buscaba conectar a las universidades y centros de investigación norteamericanos a fin de desarrollar el trabajo y la colaboración entre los científicos e investigadores.

A partir de entonces la antigua red militar empieza a ser enriquecida por los aportes del mundo civil, particularmente del mundo académico, y posteriormente del mundo empresarial, dando origen a un conjunto de innovaciones que van a explotar quince años después cuando la red es abierta al público masivo, y nace oficialmente Internet.

La base conceptual de Internet como proyecto militar, era que la red no debía ser gobernada por un cerebro o computador central. Si era controlada desde un solo punto, entonces sería vulnerable en ese lugar, por lo tanto se necesitaba una red con un amplio grado de autonomía y libertad, con cierta vida propia. La fortaleza de la red consistiría en su carácter abierto, descentralizado, hasta cierto punto caótico por la ausencia de un control único, y por la forma inteligente en que la información se movía a través de ella, buscando a su destinatario final mediante diversos caminos. Los sencillos y robustos lenguajes y códigos fueron hechos para que la red pudiese involucrar y conectar a todos los participantes sin complicados niveles de jerarquía ni problemas de compatibilidad entre equipos informáticos y dispositivos de telecomunicaciones, a fin de que pudiese subsistir, aun si una parte de ella era destruida.

Lo que no pudieron prever los creadores de Arpanet era que esa poderosa filosofía, inspirada en objetivos de carácter militar, se conservaría casi intacta 40 años después, y constituiría la quintaesencia de la más grande, extendida y controversial red de comunicación e información creada por la humanidad. Un medio en permanente evolución, un fenómeno cultural y económico que influye cada vez en mayor medida en nuestras vidas, y que presenta múltiples ventajas y no menos peligros. Su desarrollo, crecimiento y aprovechamiento para los fines de convivencia y bienestar colectivos constituye un desafío para los ciudadanos, los gobiernos, las organizaciones y la sociedad en su conjunto.

¿Qué es el WWW?

La telaraña mundial de información, o *World Wide Web*, por sus siglas en inglés, es un invento del Laboratorio Europeo de Física de Partículas (CERN). A finales de los 80, un grupo de científicos del CERN, liderados por Tim Berners Lee[8], buscando desarrollar un sistema para compartir e intercambiar información descubrieron un nuevo y accesible lenguaje que revolucionaría la Internet. La idea que los orientaba era crear un sistema de revisión de documentos visual, rápido y fácil de usar, de forma tal que cuando un investigador accediese a la información en una base de datos no tuviese que gastar tiempo mediante complicados sistemas de búsqueda, o en extensos y enredados índices. Fue así como dieron con el concepto de hipertexto. El hipertexto no era más que una señal visual, programada mediante un lenguaje especial, que marcaba un texto y le decía al usuario que detrás de dicha marca había más información. Así cualquier usuario, podía saltar o navegar de forma rápida entre diferentes documentos con sólo hacer clics en los hipertextos creados por el autor del documento.

Se podía así organizar de forma inteligente, extraordinarias cantidades de información y hacerla accesible a través de las redes a otros usuarios. La idea de hipertexto (o hipervínculo) rompía la linealidad de la lectura y de la búsqueda, suponía un sistema de manejo de información mucho más rico e ingenioso, y sobre todo, era de una sencillez impresionante, ya que se basaba en un lenguaje (HTML[9]) extremadamente sencillo de programar.

Como el lenguaje HTML permitía vincular mediante hipertextos grandes cantidades de información, el documento se podía conceptualizar como una telaraña (*web*) de información, y dado que el salto o la navegación comenzó haciéndose entre páginas de un mismo documento, se popularizó el término «página *web*» para describir el

8 Conocido desde entonces como el padre del www.

9 HTML: *Hyper Text Markup Language*, por sus siglas en inglés. Literalmente: Lenguaje de Marcadores de Hipertextos. Desde su creación el lenguaje con que se programan las páginas o sitios web, a fin de que puedan ser visualizados y accedidos por cualquier computador.

aspecto que cobraba la información al ser desplegada en la pantalla del computador.

Este descubrimiento pronto se reveló como una innovación extraordinariamente poderosa. No tardaron sus creadores en desarrollar el programa que debía instalarse en cada computador y permitía ver las páginas web desde cualquier parte del planeta. Como el usuario virtualmente navegaba en un mar de la información, a estos programas los denominarion navegadores (*browsers*).

A principios de 1990, los programas navegadores comenzaron a invadir los computadores personales. La gran mayoría fueron distribuidos gratuitamente por la red, convirtiéndose en poco tiempo en el sistema estándar para navegar y buscar información por la red. Con sus capacidades para mostrar, acceder gráficamente y de forma intuitiva a la información, la web revolucionó Internet e hizo posible su despegue comercial. Hoy en día, prácticamente todos los servicios de información que se hallan en Internet son provistos mediante sitios (*sites*[10]) web y el sencillo lenguaje desarrollado por Tim Berners Lee sigue desarrollándose, integrando capacidades multimedia, voz, video, realidad virtual, comercio, operaciones remotas, etc.

¿Qué es el comercio electrónico?

El surgimiento de la *web* dio una vida inusitada a Internet. El uso de recursos gráficos y multimedia, la navegación intuitiva y la posibilidad de organizar grandes cantidades de información y bases de datos mediante hipertextos, expandió las posibilidades de uso de las autopistas de la información. La búsqueda de nuevas aplicaciones para el Web daría otro precioso fruto poco tiempo después mediante el desarrollo de tecnologías informáticas que permitían guardar de forma segura la

10 Dada la complejidad que ha adquirido la información en el *web*, el término página *web* ha venido siendo sustituido por el de site o sitio web. Un sitio *web* es un complejo sistema de información interactivo, que incluye grandes bases de datos conectadas entre sí, y que brindan la información en tiempo real a millones de usuarios en todo el mundo.

información de los usuarios de la red, llamadas tecnologías de encriptamiento[11]. Los datos de una persona u organización (incluyendo la información financiera) podían ser escondidos mediante un código de forma tal que viajarían por la red sin posibilidad de ser interceptados o descifrados, manteniendo en secreto la confidencialidad de la operación realizada. Esta tecnología inmediatamente atrajo la atención de los bancos y las empresas operadoras de sistemas de crédito, quienes rápidamente la asumieron y desarrollaron. La posibilidad de que un potencial cliente de una empresa pudiese, ya no sólo revisar y evaluar catálogos de productos, sino pasar directamente a comprar a través de las redes teleinformáticas dió origen al comercio electrónico, es decir, la compra y venta de bienes y servicios a través de Internet, comenzó a ser una realidad.

Hay quienes afirman que el comercio en Internet nació cuando, el dueño de una pizzería en California, decidió empezar a ofrecer pizzas en su página *web*. A través de ésta, recibía órdenes en línea que luego enviaba a los poblados cercanos, mientras el cliente pagaba al momento de recibir el pedido. Sin embargo, dada la globalidad de la red (y las especiales características del producto), quedaba el problema de si la pizza era comprada desde Nueva York. El experimento, aunque exitoso, en realidad era una sofisticación de los sistemas de pedido por teléfono.

Desde la historia de la pizza digital, lo que caracteriza plenamente al comercio electrónico es que la mayor parte de la operación de compra-venta se realiza totalmente en línea (*on line*) y de forma automática, mediante la conexión de las bases de datos de vendedores, proveedores, bancos y sistemas de crédito hasta el consumidor final. El cliente entra o navega hasta un sitio de comercio electrónico, revisa el catálogo disponible, ordena la compra, provee sus datos a un sistema interconectado que revisa la operación, informa sobre la

---

11 Encriptar es el proceso general de codificación de datos con un propósito de seguridad. Las tecnologías de encriptamiento permiten «esconder» la información que viaja por las redes mediante códigos o «llaves» que sólo conocen las partes involucradas en el proceso.

disponilidad del producto o características del servicio solicitado, calcula los costos de compra más el envío (incluyendo por supuesto la ganancia de negocio virtual), chequea la existencia de fondos, y autoriza o niega la operación, sin que se produzca –hasta ese momento– ninguna intervención humana. De allí el proceso deja de ser digital y vuelve a ser analógico, es decir, involucra un sistema de búsqueda física de los productos en depósito o a terceros, y el envío mediante los sistemas tradicionales de transporte hasta el comprador final.

Por sus características, el intercambio comercial en Internet comenzó con bienes durables tales como libros, CD de música y video. Pronto, la agencias de viajes y turismo descubrieron la facilidad de hacer ventas en línea de tickets, reservaciones y paquetes de viajes. Más adelante las empresas de *software* y de computación, luego los bancos, las empresas aseguradoras y otros entes financieros que rápidamente adaptaron su oferta a los nuevos canales digitales: compra de acciones o inversiones en línea, transferencia de fondos, paquetes de seguros, asesoría financiera. Y de seguidas, cada sector de la industria empezó a hacer comercio electrónico: electrodomésticos, vehículos, alimentos no perecederos, etc. Además de la venta a consumidores finales, nació el comercio negocio a negocio[12].

Detrás de su aparente sencillez, el comercio electrónico supone sin embargo la efectiva coordinación de un conjunto de procesos digitales y físicos. La seguridad de los datos del comprador y su confidencialidad constituyen la clave del proceso. Si la operación puede ser vulnerada por clientes fantasmas, delincuentes que engañan a los sistemas o roban información financiera, o no se coordinan adecuadamente las bases de datos de crédito, bancos y vendedores virtuales, además de la confiabilidad del negocio para el cliente, el proceso puede resultar de un altísimo costo para todos los agentes involucrados.

El comercio electrónico ha sido definido como la próxima fron-

---

12 Comercio bussines to bussines (*b 2 b*) que se traduce en realizar las normales operaciones comerciales entre grandes empresas y proveedores a las redes teleinformáticas.

tera de Internet. La reducción de costos en personal, planta e inventario, que se traduce en atractivos precios para el consumidor, la velocidad de los procesos que permiten hacer compras y transferencias de fondos mediante simples intercambios de datos entre computadores, la posibilidad de abrir negocios virtuales las 24 horas, y la extensión de los mercados y clientes potenciales a casi todo el planeta, lo convierten en un factor de negocios de primer orden.

El alto atractivo y las enormes sumas que día a día se negocian vía Internet también determinan que mediante el comercio digital y las transacciones electrónicas en general se produzcan incontables delitos informáticos. Los delincuentes se mueven del mundo real al mundo virtual. El robo y falsificación de identidad financiera, alteración de sistemas de información financiera, lavado y legitimación de capitales provenientes de delitos como el narcotráfico y el tráfico de armas, la estafa mediante la creación de falsos negocios virtuales que ofrecen productos o servicios inexistentes, etc., constituyen fenómenos que abundan en la red.

LA ECONÓMIA DIGITAL: EL MUNDO EN UNA RED

Al analizar la expansión explosiva de Internet y de los fenómenos de informatización de la sociedad algunos autores hablan hoy del advenimiento de una sociedad-red, asimilando el concepto a una vieja idea de un polémico pensador de los años 70, Marshall McLuhan, quien predijo que el mundo se convertiría, por obra y gracia de los medios masivos de comunicación, en una aldea global[13].

Lo cierto es que a partir de finales de los años 80, el explosivo

13 Internet ha sido comparado a la aldea global de McLuhan por la creación de comunidades virtuales mundiales donde se borran las fronteras geográficas y culturales.

crecimiento de Internet ha configurado una realidad que va mucho más allá de lo tecnológico. Tal como lo describe la Organización de Naciones Unidas: «Escribir programas de ordenador y descubrir el código genético ha sustituido la búsqueda del oro, la conquista de la tierra y la gestión de la maquinaria como ruta hacia el poder económico. El conocimiento es el nuevo valor: más de la mitad del producto interno bruto de los países más desarrollados está basado en el conocimiento. Tanta es la importancia de estas tecnologías que las nuevas reglas de la globalización-liberalización, la privatización y los cada vez más estrictos derechos de propiedad intelectual están determinando su uso y control, con importantes consecuencias para el desarrollo humano»[14].

Para Don Tapscott, el mundo viaja hacia una nueva economía, una economía del conocimiento: la economía digital[15] cuyos rasgos principales son:

1.- Conocimiento. La economía que surge a través de las tecnologías de la información es una economía del conocimiento. El conocimiento hoy en día no es sólo un factor más de la cadena de producción, tal como el trabajo, el capital o la tierra. El conocimiento es el recurso fundamental que agrega valor a los productos. El cerebro está produciendo hoy en el mundo más valor que las manos. Ocho de cada diez nuevos empleos en los Estados Unidos se generan hoy en el sector de las tecnologías de la información. Ni siquiera la industria de la guerra o de la energía generan tal capacidad empleadora.

En los grandes mercados de valores, las empresas líderes del área de la información como Microsoft, Oracle o Yahoo, superan ya con creces en capital y valor a las tradicionales empresas productoras de automóviles, armas o bienes de consumo manufacturado. Tales empresas no tienen grandes plantas, galpones ni miles de trabajadores colocados en una cadena de producción. Generan sus beneficios de la

---

14 Informe para el Desarrollo Humano de la ONU, 1999.

15 *The digital economy: promise and peril en the age of networked intelligence*. Mac Graw Hill, 1995.

venta de productos intelectuales, de las expectativas de su crecimiento y de audaces estrategias de mercadeo.

2.- Digitalización. La nueva economía es una economía digital. Toda la información que viaja por las redes mundiales está estructurada en base a un mismo código, el lenguaje binario que permite su uso por parte de las computadoras. En forma binaria viajan hoy a la velocidad de la luz transacciones comerciales, datos personales, órdenes de compra y venta, productos de entretenimiento, noticias, sonidos, videos, instrucciones para manejar equipos a distancia, bases de datos, etc. La digitalización es el proceso central mediante el cual podemos convertir muchos de los bienes actuales en información, reduciendo los costos y haciendo reproducible, accesible y comunicable a todas partes dicha información. La ONU en su informe sobre el desarrollo humano da cuenta del proceso: «Un documento de 40 páginas se puede enviar de Madagascar a Costa de Marfil, por ejemplo, por mensajería en cinco días a un coste de 75 dólares; por fax, en 30 minutos y a 45 dólares; o por correo electrónico, en 2 minutos y por menos de 20 centavos, pudiéndose enviar al mismo tiempo a cientos de personas más sin coste extra. La elección es sencilla, y está ahí»[16].

Algunos adoradores de la cultura digital, demasiado extasiados con los bits, han pronosticado incluso la muerte de algunos objetos como los libros, por el proceso digital. La respuesta a estos apólogos la han dado los propios consumidores. Paradójicamente, desde la ampliación de las redes por el mundo, se han vendido más libros que nunca en la historia de la humanidad. Internet ha potenciado la difusión de la cultura del libro, bastante mediatizada por la hegemonía de los medios audiovisuales. Algunos autores audaces como Ernesto Sábato y Stephen King han aprovechado este fenómeno. Sus últimos libros fueron regalados durante días por Internet antes de salir impresos. El resultado final fue que ambos libros se vendieron mucho más después.

Ciertamente, la posibilidad de reproducir muchos de los bienes

16 ONU: Informe sobre el desarrollo humano, 1999.

culturales mediante su digitalización ha amenazado uno de los pilares del sistema capitalista como lo son los derechos de propiedad. La disputa actual que sacude la red y los juzgados en Estados Unidos es la aparición de un *software* desarrollado por la empresa Napster. A través del sitio de Napster en Internet, cualquier fanático de la música puede conectarse directamente con la computadora de millones de otros amantes de la música e intercambiar libremente archivos de música digitalizada. Las grandes comercializadoras de CD demandaron a Napter acusándola de violar derechos de propiedad intelectual y de producirles inmensas pérdidas, mientras varios millones de usuarios, la comunidad más grande actualmente en la red, intercambia música libremente.

3.- *Virtualización.* La nueva economía se mueve en un entorno virtual, donde la realidad no es lo que parece y donde confluyen nuevas realidades creadas enteramente por computadores mediante el uso de información. Empresas y transacciones virtuales, comunicación virtual, voto virtual, trabajadores virtuales que operan desde sus casas a miles de kilómetros de distancia de su puesto de trabajo, servicios públicos virtuales, sexo virtual. La realidad virtual crea y modifica el mundo real creando nuevos y complejos escenarios de actuación en todos los ámbitos de la vida social. La realidad se vuelve un dato manejable y operable en mundos nuevos creados dentro del ciberespacio y las redes telemáticas.

4.- *Integración y Acceso.* La economía digital que surge desde los países desarrollados y se expande por todo el mundo tiende a crear nexos entre las personas y las organizaciones. De las redes locales, científicas y corporativas estamos pasando a redes y comunidades virtuales, donde se genera e intercambia conocimiento e información entre todos los actores sociales. La expansión del correo electrónico y de la llamada Telaraña Mundial de la Información (*World Wide Web* -www) ha permitido el acceso, creando la ilusión de que todos estamos potencialmente conectados a un gran medio de comunicación. Las

posibilidades que existen hoy de comunicación internacional a bajo costo, de conocer otras culturas y de manejo de la información en grandes cantidades, desde casa y relativo control por parte del usuario, constituyen un fenómeno transformador de las relaciones humanas.

5.- *Desintermediación.* La economía de la información tiende a eliminar los mecanismos de intermediación característicos de la economía industrial. El acceso directo a muchas fuentes de información, datos, negocios y servicios permite desbloquear parcialmente el control de los intermediarios (llámense revendedores, mayoristas, partidos políticos, gremios, etc.) reduciendo costos y permitiendo un flujo más directo de comunicación. Los ciudadanos pueden pagar impuestos, hacer quejas de forma más directa a los organismos públicos y esperar respuestas más rápidas que a través de la gestión de un partido político o grupo de interés. Las empresas pueden tratar directamente con sus clientes y proveedores bajando los costos de información y de transacción. Los consumidores pueden comprar directamente en planta negociando mejores precios.

6.- *Innovación.* La permanente mejora de los productos y servicios, constituye uno de los ejes de un entorno económico dominado por la cultura digital. Existe una fuerte presión para reinventar lo que circula por la red, lo cual significa, por otra parte, una revalorización de la educación, la capacitación y la formación del recurso humano. Mientras la industria automotriz en países como Japón y Estados Unidos asumen un ciclo de obsolescencia para los vehículos de dos años, tales ciclos para algunos productos electrónicos, ya se calculan en tres meses. Un nuevo chip o cerebro de computadora, que por lo general duplica la velocidad del modelo anterior, se crea cada seis meses con un precio casi de la mitad. Algunos productos financieros tienen un ciclo de vida de unos pocos días u horas. Ciertas empresas de informática han llegado a introducir hasta 500 nuevos productos en un año, pero como dice el propio Bill Gates «no importa cuán bueno sea su producto, usted tiene sólo 18 meses

para no fallar».[17]

7.- Masificación personalizada. Aunque parezca mentira, la economía digital permite algo que la economía masificada industrial no ha podido alcanzar: generar productos en masas pero adaptados a los gustos y necesidades personales. La versatilidad del medio digital y su facilidad de uso mediante computadores permiten la creación de un espacio personal en la red para cada cual. Hoy en día se puede buscar la información, comprar, vender y negociar de acuerdo a las necesidades específicas de un grupo o segmento. Los ciudadanos adquieren su propio espacio en la red a través de páginas personales donde comparten con amigos y personas de gustos similares sus intereses particulares.

8.- Inmediatez. El acceso inmediato a bienes, servicios e información, la reducción de los tiempos de entrega y de inventarios (la filosofía justo a tiempo) permite a la nueva economía cambiar los modelos de negocios y de comunicación. Los productos se empiezan a fabricar al momento y de acuerdo a las demandas específicas del comprador, como hacen ya algunas empresas de automóviles donde a través de una página en Internet el futuro comprador puede diseñar su propio vehículo. Muchas empresas están empezando a operar mediante el sistema «cero inventario», gracias al mejoramiento de los procesos de envío que han estimulado las tecnologías de información. El acceso e intercambio de datos se produce instantáneamente, permitiendo una comunicación más efectiva en los procesos educativos y de investigación.

9.- Democracia. Mientras que en la comunicación y difusión masiva tradicional (la televisión, el cine, la radio) los flujos de información, salían desde unos pocos centros hacia una periferia pasiva, de arriba a abajo, sin posibilidad de respuesta, en la red, todos pueden teóricamente ser emisores y receptores. La inversión o modificación de la relación

---

17 Bill Gates. *The road aheads* (Camino al futuro).

tradicional entre emisor y receptor dentro del proceso de comunicación le da a Internet su carácter democrático, participativo y hasta cierto punto revolucionario. Medios como video conferencias, las charlas interactivas y bibliotecas virtuales, permiten el acceso masivo a fuentes de información y generación de nuevo conocimiento. La democracia también se manifiesta en una relación más directa, por ejemplo, entre gobierno y ciudadano. La digitalización de los servicios públicos en el sentido de permitir a la gente participar en el diseño, procesos de presupuestación y control de los servicios, es una muestra de las aplicaciones de la red para fines de democratización.

10.- Globalización. La proyección de Internet en la vida cotidiana, en el consumo, en la universidad, en el aprendizaje, en el trabajo, en el ocio, o en las comunicaciones personales, la convierten, sin duda, en el fenómeno más contemporáneo y en la expresión más clara de la globalización. Los fenómenos de la red no respetan las fronteras: un evento en un país puede tener un impacto inmediato en otro, debido a la velocidad con la cual fluye la información y a causa de la forma dramática en la cual puede ser presentada. Los eventos, asuntos y problemas no pueden ser más contenidos en un país o en una región. Si son significativos, se vuelven eventos globales, asuntos globales o problemas globales. La globalización es quizás una de las características más visibles de la red. Ante esta realidad tienden a surgir de un lado actitudes pasivas que asumen acríticamente el fenómeno sin evaluar su impacto en la realidad cultural específica de un país o de una comunidad. Otras veces, surgen prejuicios descalificadores que tampoco entienden el fenómeno y por tanto lo hacen inmanejable socialmente.

La pérdida de control de ciertas actividades de los jóvenes, creciendo en un entorno de red, la promoción de una cultura de la violencia, de contenidos delictivos, son realidades a las cuales no podemos escapar. Por otra parte, la red ha abierto posibilidades de expresión a movimientos políticos y sociales que no tienen cabida en los medios masivos como la televisón debido a intereses económicos o geopolíticos. Las páginas de los zapatistas mexicanos ayudaron en gran parte a

lograr que el mundo entendiera su lucha. Lo mismo ha sucedido a nivel ambiental con la famosa campaña anti MacDonald's que permitió difundir información ignorada por millones de consumidores en el mundo, o la acción de guerrilla informativa por Internet de Radio B-92 en Belgrado, burlando los controles de la férrea dictadura de Milosevic.

La globalización de la información y las comunicaciones son un fenómeno complejo. En la misma medida que ofrece herramientas al ciudadano común, a las minorías, a los marginados, herramientas impensables hace algunos años, en esa misma medida genera peligros como la vacuidad de contenidos o la distorsión de los valores democráticos, así como da espacio al delito y al abuso.

EL ESTADO FRENTE A LA RED: UN DESAFÍO DE POLÍTICAS PÚBLICAS

Los cambios tecnológicos radicales deberían conducir a planteamientos y redefiniciones políticas igualmente radicales. Como institución democrática, como más que un simple árbitro de lo social, como agente activo cuya responsabilidad es el bienestar, la equidad y la justicia social, el Estado democrático en América Latina debe comprometerse a pensar el fenómeno de la Era de la Información y de la Economía Digital, como algo más que un fenómeno tecnológico o informático.

Desde esta óptica, Internet y los fenómenos sociales, culturales y económicos que se producen a través de las redes de información, deben enfocarse como un problema de políticas públicas. Un asunto que requiere algo más que una actitud de pasivo asombro, de ciego rechazo o de ignorante aceptación. Ciertamente, la tecnología de la información puede jugar un rol vital en nuestros países ya que puede ayudar a mejorar la educación, la capacitación del recurso humano y el acceso a las fuentes de información que pueden elevar la capacidad competitiva de nuestras economías y de nuestros ciudadanos. Consecuentemente, las redes digitales, que permiten organizar y controlar

mejor los flujos de información y los procesos administrativos entre los actores sociales, pueden mejorar la efectividad del gobierno en la provisión de servicios públicos tales como la distribución de alimentos, medicinas, y los programas de participación comunitaria.

La sociedad latinoamericana en su conjunto afronta hoy el reto de las nuevas tecnologías de la información, sin que aún la región haya podido integrarse efectivamente al circuito de las economías industrializadas. Los problemas estructurales como la fragilidad de las economías regionales, la ausencia de una infraestructura tecnológica y de telecomunicaciones, el rezago educativo, en ciencia y tecnología, la falta de una cultura teleinformática en el ciudadano, y los vacíos legales, ubican a la región en calidad de un participante pasivo, mercado consumidor de los nuevos productos digitales, más que como un participante activo, generador de bienes y servicios. Aunque la red mundial abre oportunidades a nuevos sectores, (incluso algunos optimistas nos ven como la próxima frontera virtual) la verdad es que el interés por América Latina se encuentra hoy en su característica de ser consumidor y no productor en el nuevo sistema de las tecnologías de información.

Es cierto que en los últimos diez años América Latina se ha comenzado a incorporar a la economía mundial de la información. El uso de computadores ha crecido significativamente, la estructura de telecomunicaciones se encuentra en plena expansión y la apertura de las telecomunicaciones ha avanzado en los principales países de la zona. Mientras tanto, crece el acceso y uso de Internet de forma acelerada, se digitalizan bases de datos, se tienden redes de fibra óptica entre las ciudades, se instalan satélites en la región y se expande el uso del castellano por la red.

Estos hechos, sin embargo, configuran un panorama actual todavía modesto si se los compara con las cifras reales. Hasta comienzos de 1999, por ejemplo, de un total de 335,8 millones de latinoamericanos, sólo 3,4 millones usaba computadores, es decir, un 3,4%; de ellos 1,5 millones de argentinos, 6,7 millones de brasileños, 900 mil chilenos, 3,6 millones de mexicanos y casi un millón de venezolanos.

Menos de tres ciudadanos latinoamericanos de cada 10 que usaban computadora, estaban conectados a Internet, es decir, un total inferior a los dos millones de personas[18].

Como contrapartida, las proyecciones muestran que el crecimiento del sector de las tecnologías de información en Latinoamérica será mayor que en cualquier otra región del mundo en los próximos cinco años, y mayor que cualquier otro sector económico en la región, incluyendo el petróleo o el narcotráfico. Para comienzos del año 2000 se esperaba ya que el número de usuarios de Internet superara los 7,3 millones, un crecimiento de más del doble respecto al año anterior, y se proyecta que habrá entre 27 y 34 millones de internautas en toda América Latina para el 2004.

Los estudios también predicen, entre otros hechos, la reducción violenta de los costos de conexión telefónica y de Internet, y la ampliación de las redes físicas (fibra óptica, conexiones satelitales, servidores, etc) producto de la competencia producida por la apertura de las telecomunicaciones. La lucha por el mercado latinoamericano producirá en la región una cuantiosa inversión de recursos que expandirá las posibilidades de comunicación, el comercio electrónico y diversificará la oferta de productos digitales en la zona[19].

Algunos fenómenos como el comercio y las transacciones electrónicas plantean un verdadero desafío a la imaginación del sector público. Aunque son ciertas algunas de esas historias románticas acerca de las empresas latinoamericanas que venden artesanías por Internet directamente en los grandes mercados del norte, la verdad es que el balance en estos momentos no nos favorece. América Latina es visto como un potencial mercado consumidor de bienes y servicios producidos en la economía digital. Según un informe de la empresa Boston Consulting Group, los consumidores latinoamericanos, ciudadanos de clase media y empresas medianas y grandes, gastamos

---

18 Lehman Brothers. *The Internet and Latin America. The next virtual frontier*. August, 1999.

19 *Ibídem*.

aproximadamente unos 459 millones de dólares mediante comercio y transacciones electrónicas en 1999, más de la mitad en empresas virtuales ubicadas en los Estados Unidos[20].

Estas predicciones y hechos deben llamar a la reflexión a los estados y gobiernos latinoamericanos. La violenta incorporación a un proceso de naturaleza tan compleja generará consecuencias imprevisibles tanto en la economía como en la cultura de la región. Los beneficios, inmensos sin duda, traerán aparejados costos inimaginables. Mientras cada día, una cantidad creciente de ciudadanos latinoamericanos acceda a la red, intercambie e interactúe con los sistemas de información, más formación y capacitación se requerirá, y más rápida deberá ser la reforma educativa. Mientras el acceso brindará posibilidades extraordinarias para la colaboración cultural, científica y la integración regional y con el mundo, el reto será preservar las identidades propias y evitar las tendencias como la homogeneización cultural, el consumismo tecnológico, la vacuidad de los contenidos y la sobresaturación de información.

El acceso traerá consigo también los clásicos problemas de inseguridad informática: invasión de la privacidad, intervención de sistemas y bases de datos, y terrorismo informático, entre otros. Mientras más transacciones y negocios digitales se generen en y desde América Latina, más posibilidades de delitos tales como estafas, fraudes informáticos, robo de información, violación de derechos de propiedad, y lavado de dinero estarán a la orden del día, afectando negativamente a los ciudadanos y a los agentes económicos.

Potencialmente, se espera que la teleinformación ayude a aumentar las posibilidades de nuestros pueblos de alcanzar mayores niveles de prosperidad. La sociedad de la información demandará en el futuro próximo en América Latina nuevos servicios de comunicaciones, y la instrumentación y operación de dichos servicios exigirá una cuota relevante de inversiones y de recursos humanos capacitados. Al mismo tiempo, tal como funciona la economía digital, toda inversión

---

20 *Ibidem.*

en comunicación genera mucho más valor agregado. Las inversiones que se realizan y las que se realizarán en los años por venir influirán de forma importante en la modernización de la sociedad latinoamericana a través de efectos multiplicadores sobre su economía y de efectos transformadores de los hábitos de comportamiento social. Las redes de los servicios públicos, la fibra óptica o los satélites entre otros recursos, por ejemplo, poseen múltiples aplicaciones y usos de acuerdo a las realidades del mercado y a las políticas que fijen los gobiernos para aprovechar social y productivamente estas inversiones. Dependerá de políticas de Estado el que esa infraestructura sirva a la sociedad en su conjunto, y no sólo a ricos y poderosos.

En Venezuela, el desarrollo del sector de la teleinformación es clavé para que nuestro país se incorpore al siglo XXI. Todo lo que ha dejado de hacerse en esta área tendrá que hacerse en los próximos años para no quedar rezagados. Redes educativas, redes de servicios públicos, legislación moderna y flexible, regulación y control de los suprapoderes tecnológicos, estímulo a la participación, capacitación y acceso. Las tareas son múltiples y los retos inmensos.

Para que Venezuela se incorpore efectivamente al siglo XXI es imprescindible, en primer lugar una política de democratización del acceso, difusión y promoción de la cultura teleinformática. Por el lado del Estado significa entre otros aspectos, crear y promover el desarrollo de una infraestructura de telecomunicaciones que sirva de soporte al acceso público de una forma segura y estable. En esta área no bastaría sólo con una apertura de los mercados, condición necesaria pero no suficiente. No debe olvidarse que Internet fue desarrollado durante más de 25 años por el Estado norteamericano, como una política estratégica de seguridad y desarrollo del conocimiento. Cuando se habla hoy en la literatura digital acerca de la columna vertebral (*back-bone*[21]) de Internet, se olvida que fue una creación del sector público que conecta a los principales centros de investigación y universidades

21 Estructura básica de comunicación, la red básica sobre la que se monta Internet y está conformada por cuatro grandes nodos o puntos ubicados en universidades norteamericanas.

de los Estados Unidos, sin el cual hubiese sido imposible el crecimiento posterior de la red.

El Estado venezolano debe avanzar en una política de desarrollo de redes e infraestructura para las tecnologías de información, apoyándose en el sector privado. Debe apoyar y estimular la democratización del acceso al público, creando a nivel educativo y comunitario puntos y espacios de conexión que permitan a los ciudadanos de bajos recursos acceder a la red. Debe plantearse la reducción de los costos de conexión a las redes mundiales, mediante políticas de tarifa plana, como se ha hecho en los países avanzados, al tiempo que debe promover una cultura de participación comunitaria y estimular el desarrollo de contenido local y servicios públicos mediante el uso de las redes telemáticas.

Pero también el Estado está obligado a legislar en el área del sector de las tecnologías de información para evitar que el uso irresponsable o delictivo de las redes se convierta en un problema para los ciudadanos, la economía y la sociedad en su conjunto. Los problemas de propiedad, delincuencia y abuso en la red son tan recientes que apenas ahora la legislación mundial está respondiendo a tales desafíos. La expansión y uso de los medios electrónicos de pago (tarjetas de crédito, de débito, chequeras digitales, etc.) que se usan en las redes de información para realizar transacciones económicas constituye en esta materia un punto fundamental de la necesaria modernización legislativa.

Para responder adecuadamente al fenómeno del impacto que están produciendo y seguirán produciendo las tecnologías de la información, los Estados latinoamericanos deben repensar el fenómeno y en cierta forma, reinventarse a sí mismos. Para ello, habrá que derribar algunos mitos teóricos y prejuicios políticos. La tecnología no debe ser vista como un enemigo, una suerte de perversa quintacolumna de los intereses mercantiles, sino como una herramienta de progreso en la medida en que sirva a toda la sociedad. La tecnología puede estar al servicio del ser humano si éste se propone manejarla y gestionarla de forma transparente, responsable y creativa. La sociedad latinoamericana

puede usar la teleinformación como herramienta poderosa para ayudar al progreso y no para abrir o profundizar brechas económicas, sociales o culturales.

Sólo en esa medida estaremos en capacidad de adentrarnos en el mundo de las tecnologías digitales, en la seguridad de que su expansión y desarrollo servirá a la sociedad para crecer y fortalecerse y no para dividirla más mediante la brecha tecnológica o digital.

Delitos informáticos: amenazas desde el ciberespacio

Junto a sus múltiples e innegables aspectos positivos, las tecnologías de la información plantean, sin duda alguna, desafíos extraordinarios para la sociedad democrática. Internet y las redes telemáticas han hecho realidad un viejo sueño: la promesa de un acceso ilimitado y relativamente democrático a la información y a los medios para producirla e intercambiarla. Cuando el ex vicepresidente norteamericano Al Gore popularizó el término autopistas de la información (los españoles las llaman las infopistas o infocarreteras) lo que quería decir es que, así como las vías de comunicación terrestre abrieron paso al desarrollo industrial, las redes teleinformáticas abrirían nuevos caminos a la sociedad en los años venideros.

Hoy, por estas superautopistas, circulan millones de personas y grupos. Ciudadanos comunes junto a grandes empresarios, niños y adolescentes al lado de partidos políticos, amas de casa junto a científicos, pero también delincuentes, terroristas, mafias organizadas y toda clase de antisociales. Todos viajando a distintas velocidades, con distintos puntos de partida y llegada y con diferentes objetivos para su viaje. Como en toda vía pública, en las autopistas de la información ronda también la inseguridad.

Al hablar de seguridad en el entorno digital no se trata sólo, como se cree, de mantener a buen resguardo la información financiera y las transacciones, sin duda uno de los aspectos más visibles del problema. Cada día un mayor número de empresas y organizaciones del sector público dependen en su funcionamiento, administración y operaciones de los sistemas informáticos y de la interconexión de complejas bases de datos que intercambian y procesan información. Los sistemas de control aéreo, los registros de contribuyentes o de

información de los ciudadanos que permiten el funcionamiento de muchos servicios públicos, y hasta los propios sistemas de seguridad y defensa, por citar sólo algunos, dependen cada vez más de las redes de datos y de la información computarizada.

La explosiva expansión de Internet, ha permitido que cada vez un mayor número de personas acceda a datos de otros y exponga su propia intimidad a la vista de los demás. La información personal, los gustos de consumo, el nivel de ingreso, los registros médicos, la vida íntima en buena parte, circula hoy por las redes sin controles y sin reglas. En esto, cautos e incautos compartimos el mismo saco virtual. Nuestros computadores pueden ser invadidos en cualquier momento sin previa autorización. Nuestra vida puede ser alterada de forma remota. Al tiempo que potencia nuestras capacidades y posibilidades, la conexión a la red de una u otra forma nos hace más vulnerables.

En la aldea global debemos pues enfrentar amenazas globales. Como la vida misma, las redes engloban la maldad y la bondad, la cooperación junto al afán de lucro, la solidaridad al lado del fraude. Desde los secretos corporativos a la privacidad, desde la violación de los derechos de autor al fraude mediante medios informáticos, desde el saboteo de sistemas de seguridad hasta la destrucción informática, los riesgos y amenazas a que nos enfrentamos son nuevos, complejos y variados.

El espacio virtual es definitivamente terreno fértil para el delito, o para decirlo de otra manera, territorio ya conocido por los delincuentes del mundo real, y absolutamente desconocido para los gobiernos. La virtualidad de los fenómenos digitales, la desaparición de las fronteras físicas, la manipulación remota de los sistemas informáticos, la asincronicidad de los procesos y la propia flexibilidad de las tecnologías de la información, constituyen rasgos que dificultan su control por parte de las autoridades y abre campo a la más dramática inseguridad.

El aumento de los delitos cometidos en el ámbito informático es hoy un hecho reconocido de forma unánime como una amenaza grave para la sociedad, no sólo en los países más avanzados sino también en aquellos que se apresuran por incorporarse a la carrera tecnológica

o que se encuentran, como Venezuela, en el inicio de un proceso de apertura de las telecomunicaciones. De hecho, el reconocimiento de que los sistemas de información son un campo propicio para el surgimiento de las más variadas conductas delictivas ha llevado a la conceptualización de toda un área de investigación penal relacionada con los delitos informáticos, denominada en algunos predios como Computer Crime o Computer Related Crime y en otros como Cybercrime, o ciberdelitos.

¿Hasta dónde tales ideas son fruto de la preocupación, y hasta dónde son fantasía o exageración? Una encuesta realizada en el año 2000 por el Buró de Investigaciones Federales de los Estados Unidos, el todopoderoso FBI, reveló hasta qué punto el delito ha penetrado los espacios cibernéticos en el país más avanzado tecnológicamente del planeta. En dicha encuesta más de un 90% de las grandes empresas reconoció constantes fallas y brechas de seguridad en sus sistemas[1]. Siete de cada diez dijo que en algún momento sus sistemas habían sido penetrados de forma no autorizada. El mismo FBI calculaba que en los EEUU las incursiones virtuales delictivas les produjo a las empresas pérdidas de más 265 millones de US $ en el año 2000, mientras que el espionaje o robo de información privilegiada a través de Internet les ocasionó otros 66 millones de US $ en pérdidas.

Por si fuera poco, sólo las empresas encuestadas perdieron además 55 millones por fraude financiero y otros 27 millones por sabotaje de sistemas en el 2000. Lo más interesante de esta revelación, es que el 59% de las empresas consultadas citó su conexión a Internet como el blanco más frecuente por donde son atacados, mientras que otro 38% afirmó que los ataques vinieron desde dentro de sus propias organizaciones. Sólo la categoría de fraude financiero aumentó un 38% entre 1999 y el año 2000. A pesar de lo grave que nos parezcan, estas cifras sin embargo puede que estén exageradamente minimizadas

---

1 Citado por Steven Phillipson. Taller de *Prevención de Fraudes. Una apreciación global de los delitos electrónicos en el siglo XXI*. Puerto España, Trinidad, noviembre del 2000. Traducido por la Fundación EnCambio.

o distorsionadas. Ciertos medios de prensa han informado que los fraudes y otros delitos informáticos le producen a la economía norteamericana pérdidas globales de más de 42 mil millones de dólares anuales.

Como lo definió un grupo de expertos de la Organización para la Cooperación Económica (OCDE) en París en 1983, el delito informático puede ser conceptualizado como «cualquier comportamiento antijurídico, no ético, no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos»[2]. En realidad, no existe un único delito informático, sino un complejo conjunto de conductas de muy diversos signos, que pueden ser calificadas como tales.

Por su naturaleza, influencia y poder, las redes telemáticas y los sistemas de información configuran al mismo tiempo, tanto un nuevo medio susceptible de ser usado para delinquir como un campo propicio para el surgimiento o refinamiento de conductas delictivas tradicionales. Lograr la tipificación y diferenciación de estas conductas delictivas tiene una trascendental importancia para determinar la ley aplicable a cada caso en particular, para crear los instrumentos jurídicos adaptados a las nuevas realidades y nuevos rostros del delito, o si es el caso, reformar los Códigos Penales. Esa tarea permitirá garantizar a los usuarios la seguridad y privacidad a la que tienen derecho, sin que se obstaculice el desarrollo de las comunicaciones como elemento de progreso social. Sin duda, el problema representa uno de los desafíos de políticas públicas más importantes que hayan enfrentado los Estados y los gobiernos en los últimos años.

---

2 Ulrich Sieber. *Documentación para una aproximación al delito informático* en *The International Handbook on Computer crime* - Computer Related Crime, 1986.

DELITOS INVISIBLES

Debido al poder que brinda la mediación tecnológica, a sus costos decrecientes y al carácter desregulado y en muchos casos anónimo del mundo virtual, los medios informáticos y las redes como Internet constituyen un vehículo perfecto para cometer delitos. En cierta forma, los medios telemáticos abaratan los costos de la actividad delictiva ya que permiten que ésta pueda ser realizada de forma remota y asíncrona[3]. Las pruebas, los rastros o huellas no son siempre fáciles de recolectar, lo que reduce los riesgos para los infractores y dificulta la tarea de quienes deben combatirlo.

Hoy en día, este tipo de delitos conforma un auténtico monstruo de mil cabezas, cuyos efectos sobre la economía, los negocios y la vida privada pueden llegar a ser tan invisibles como devastadores. La categorización de los diversos delitos informáticos es compleja y difícil. Pareciera que cada día, al ritmo que se expanden las innovaciones electrónicas surge una nueva forma de usar los recursos telemáticos para obtener beneficios ilícitamente o cometer todo tipo de acciones fuera de la ley. Repasemos aquí algunos de los fenómenos delictivos más conocidos hasta los momentos.

HACKERS, LOS CORSARIOS DEL CIBERESPACIO

El acceso a distancia y no autorizado a un sistema de procesos de datos, no cometido con fines de manipulación fraudulenta, de espionaje, ni de sabotaje sino sencillamente por diversión, curiosidad u ocio es descrito por Ulrich Sieber como una forma de «hurto de servicios», y define la actitud clásica del conocido hacker, pirata informático o de la

---

3 La asincronicidad implica que pueden efectuarse tareas de forma programada sobre una red o sistema para ser ejecutadas en tiempos diferentes. El carácter remoto supone la manipulación a distancia de sistemas e información. Es natural que ambas características faciliten el uso ilegal de dichas herramientas y dificulten su control por parte de las autoridades.

red. Este nuevo delito ha logrado su propia caracterización criminológica como delito de pantalones cortos (*short pants crime*) debido a que es cometido por lo general por jóvenes entre los 15 y 25 años de edad, de un nivel socioeconómico estable y de formación académica. Comenzó hace ya casi treinta años con el acceso y manipulación de las claves telefónicas de grandes compañías, que permitían a estudiantes universitarios hacer llamadas de larga distancia de forma gratuita, y ha terminado conformando un extensa red de personajes que circulan por las autopistas de información, cometiendo las más variadas faltas y travesuras informáticas.

Sin embargo, que tales faltas no sean muchas veces cometidas con fines abiertamente delictivos no significa que sus consecuencias no sean relevantes, puesto que pueden ocasionar destrucción de datos, bloqueos de sistemas, costos en términos de reparación de daños y pueden abrir boquetes en los sistemas que permitan la comisión de posibles fraudes financieros u otros delitos. Por otra parte, los verdaderos delincuentes informáticos se nutren generalmente de los hallazgos e innovaciones de los hackers y no pocas veces los usan o contratan para sus operaciones.

La cultura del hacker tradicional, comprende una compleja red de valores en la que se mezclan una cierta tradición de rebeldía, inconformismo y filosofía nueva era, todo ello mezclado en una suerte de consumismo y ética electrónica que ellos mismos han denominado *cibercultura*. Hakim Bey, de quien se cree que se llama Peter Lamborn Wilson, escritor, poeta y filósofo, es uno de los padres del movimiento. Ganó fama al desarrollar en los años 70 la Teoría de las Zonas Autónomas Temporales (TAZ), desde entonces uno de los credos de los grupos rebeldes que actúan en y desde Internet[4].

---

4 Uno de los textos famosos de Bey expresa parte de esa filosofía vital: «Hay un "mercado libre" de información –pero no necesariamente hay libertad para ninguna otra cosa que no sea la información–, igual que hay un mercado libre para el dinero pero no hay ninguna libertad para cualquier otra cosa que no sea el dinero. Ahora bien, los seres humanos no son "información" excepto de manera metafórica. La comida no es "información". El placer no es "información". La vida no es "información". De manera que cuando el universo es concebido sólo como información, es mucho lo que se está quedando fuera...» Hakim Bey. *Carta a Valencia*. Noviembre de 1999.

La prensa, el cine y la publicidad han convertido a los hackers en uno de los estereotipos más conocidos del medio de las tecnologías de información[5], debido al modo particular en que actúan, muchas veces por simple diversión o reto, como entrar y alterar los archivos de una gran corporación, jugar bromas a los bancos, hacer campañas políticas, etc. Los famosos «Club del Caos Informático» de Hamburgo, o el «414 Gang» de Milwaukee, cuyos miembros ya en 1983 lograron entrar a la base de datos del Laboratorio Nacional Los Alámos de EE.UU (nada más y nada menos donde se desarrolló la bomba atómica) demuestran hasta dónde pueden llegar los hackers en sus excursiones digitales por los sistemas teleinformáticos.

Clubes especializados, revistas de informática, sitios de conversación (*chats*) sobre temas de software y grupos de noticias muy particulares donde se debate desde asuntos de ética hasta trucos de programación, conforman algunos de los medios creados y mayormente frecuentados por los hackers. Personaje odiado por algunos y reivindicado por otros, lo cierto es que el hacker conforma un tipo cultural creado por el desarrollo de los medios digitales. Su influencia no es poca en la vida de los enchufados a la red, y aunque no todos usan sus conocimientos para delinquir, otros constituyen una verdadera amenaza directa o indirectamente.

TRABAJANDO CON EL ENEMIGO

A despecho de la idílica imagen anterior, Steven Phillipson afirma que aunque siguen existiendo los «hackers por placer» y los «hackers

---

5 En muchas películas el hacker es presentado como un símbolo de una nueva forma de rebeldía, un fanático que vive aislado en una suerte de religión digital, convive en un medio marginal, ama la música «tecno», coquetea con las drogas y expresa una actitud de rechazo a la sociedad de consumo. Es una suerte de héroe posmoderno y postindustrial, a veces ingenuo a veces travieso, que juega a crear un nuevo mundo mediante el uso de las computadoras. Algunas películas como la famosa *The Matrix* (La Matriz), presentan al hacker incluso como una nueva versión del «elegido», personaje destinado a luchar por la humanidad en un mundo futurista dominado por las computadoras.

políticos»[6] hoy en día una de las especies más peligrosas la constituyen los «hackers internos», es decir empleados, contratistas o consultores de las propias empresas. Su acceso y conocimiento de los sistemas y códigos de seguridad les permite causar un mayor daño con menos esfuerzo que el invasor externo, que se enfrenta al reto permanente de violentar informáticamente los sistemas. En Gran Bretaña se calcula que 75% de los robos y fraudes ocurridos en el sistema financiero son ocasionados por su propio personal, un hecho que la mayor parte de las empresas y bancos tratan de ocultar por temor a las consecuencias en pérdida de credibilidad y clientes, y por el temor subsecuente a estimular a otros hackers a actuar contra la organización.

El arsenal de armas creadas por los hackers es tan extensa y variado, que es difícil encontrar una clasificación comúnmente aceptada. Amparados en la complejas técnicas de la programación y en un conocimiento especializado, muchas de estas armas son usadas con frecuencia para alterar sistemas y procesos de datos frente a los ojos de las víctimas, mientras éstas apenas lo notan.

Entre el vasto repertorio de herramientas y prácticas creadas por los hackers se encuentran recursos informáticos que pueden «cazar» las claves o contraseñas de seguridad de un sistema, alterar los códigos originales de los programas de sus víctimas –lo cual les permite su completa manipulación– producir virus que se autorreplican causando anomalías, en muchos casos irreparables, a los datos y a los propios sistemas, bombas digitales que se programan para estallar en un determinado momento, alteración de la lógica de programas mediante la saturación de información, robo de contraseñas, simular la identidad

---

6 Un ejemplo del primer tipo sería el de un adolescente galés que obtuvo de forma ilegal la información de más de 26 mil tarjetas de crédito y las difundió por Internet. Aunque no cobró por ello, esta «travesura» costó más de 1.8 millones de libras esterlinas por compensación debido a posible fraudes cometidos con esta información, reparación de sitios en Internet y reemplazo de tarjetas. De los hackers políticos recuerda Phillipson las incursiones de hackers serbios que durante los recientes conflictos en la ex Yugoslavia invadieron constantemente páginas de relevantes empresas colocando el mensaje «Kosovo es Serbia». Recientemente el conflicto palestino-israelí y la lucha entre los anti y pro ETA en España han llevado sus frentes al mundo virtual de la Internet.

de otro, hasta recoger y usar la «basura electrónica» –los datos que quedan flotando en los sistemas y discos– con fines diversos.

VIRUS INFORMÁTICOS

La idea más común es la que define a los virus como software usado para destruir datos en un computador[7]. Una vez que el programa se ejecuta, el código del virus también se activa y agrega copias de sí mismo a otros programas y áreas del sistema. Analógicamente a su funcionamiento en el cuerpo, los virus se «reproducen» o «replican» dentro del sistema cada vez que se ejecutan los programas infectados, logrando paulatina o violentamente alcanzar cada vez una mayor cantidad de datos.

Una de las especies de virus más conocidas son los llamados programa gusano (*worm*[8]), los cuales se copian a sí mismos en el disco y la memoria, consumiendo progresivamente los recursos de los computadores y eventualmente dañando significativamente el sistema.

Los virus constituyen en sí mismos toda una subcultura dentro de la naciente sociedad de la información. Se les ha utilizado para lanzar ataques contra sistemas y bases de datos de empresas y organizaciones por motivos económicos y hasta políticos. La mayoría de los creadores de virus lo ven como un hobby, algunos los usan como un medio de propaganda o difusión de sus quejas o ideas radicales; otros crean virus cada vez más destructivos y difíciles de controlar por el orgullo o la competitividad que existe entre los programadores; y hay quienes lo usan como medio de sabotaje. Pero independientemente de la motivación, la verdad es que cada día la mayor interconexión de los sistemas y bases de datos en el mundo hace que la difusión de cada

---

7 Alan Freedman. *Diccionario de Computación*. McGraw Hill. Después que se escribe el código del virus, se oculta en un programa existente.

8 Existen otras acepciones para la palabra «worm» en el medio informático no vinculadas a los virus. Véase Alan Freedman, Ibídem.

nuevo virus se convierta en una verdadera epidemia, generando en algunos casos auténticas oleadas de pánico informático.

Un ejemplo reciente sucedió el año pasado con la difusión del famoso virus del amor (*I love you*), un poderoso programa de destrucción de datos que llegaba a los buzones de correo electrónico de las víctimas con el mensaje «Te amo». Aquí nuevamente el ingenio de los programadores de virus generó un caos mundial por los terribles efectos que la difusión masiva e inocente del virus logró por Internet.

LA INTIMIDAD DE TODOS

Como afirma Don Tapscott[9], «la red tiene el escalofriante poder de destruir la intimidad de una forma irrevocable que carece de antecedentes». En las sociedades modernas resulta frecuente que los ciudadanos crean que tienen el derecho a decidir qué información personal divulgan, a quién y con qué fines. Se acepta, no siempre de buena gana, dar detalles de la vida personal a organismos del Gobierno (registros civiles, judiciales y de impuestos) y a empresas como los bancos con el fin de acceder a servicios, préstamos, etcétera. El ciudadano piensa por lo general que la información sobre sí mismo forma parte de su patrimonio personal, afirmación de su identidad y garantía de su libertad. Al menos ésa ha sido una de las promesas de la democracia con su preceptos acerca de la inviolabilidad de la vida personal... hasta que llegaron los medios digitales.

Sin control, asegura Tapscott, la red y los medios telemáticos en general podrían hacer que esa idea fuese una mera ilusión. «A medida que las comunicaciones humanas, las transacciones comerciales, el aprendizaje y el juego se van incorporando a la red, cantidades y tipos inimaginables de información se van digitalizando y difundiendo por las redes. ¿Cómo podemos proteger la intimidad en una economía digital?»[10].

---

9 Don Tapscott. Prólogo a *La Red* de Juan Luis Cebrián. Santillana Editores, 1998.
10 Don Tapscott. *Ibídem.*

Otros autores como Juan Luis Cebrián dan cuenta de lo que ya es una realidad cotidiana: «una de las características del ciberespacio es la facilidad con la que uno puede ser asaltado, no ya cuando pasea por el mismo, sino, incluso, cuando está tranquilamente en casa... No existe ninguna seguridad respecto a lo privado de los intercambios, sean económicos, amorosos o de cualquier otro género, salvo que se utilicen sistemas de codificación y cifra».[11]

Cebrián atribuye este hecho a lo que llama el carácter informal, autoorganizativo y caótico de las redes, que las hacen vulnerables a cualquier intervención. Se trata de una realidad imposible de ignorar. En las redes de información, llámense éstas Internet o redes locales, la intimidad está más expuesta que nunca. Se trata de un problema cuya obviedad a veces impide su clara percepción por parte de las autoridades, paradójicamente muy interesadas en controlar los contenidos que circulan por la red, pero poco atentas a lo que en la red se hace con la información de cada individuo.

Por una parte, los administradores u otras personas autorizadas para acceder a los grandes computadores o servidores, en los cuales se localiza la información, los programas o aplicaciones, pueden obviamente acceder a nuestro buzón de correo electrónico y ver quién o qué se nos escribe, qué decimos en nuestras comunicaciones virtuales con familia, amigos, negocios o desconocidos.

Un peligro adicional lo encarnan los hackers, piratas u otros usuarios de las redes que pueden rastrear la información mediante programas especiales (software que se comercializa o se consigue gratis en la propia Internet). Y del otro se encuentran aquellas personas o empresas que han hecho de la comercialización no autorizada de la información personal, un negocio redondo en Internet.

Este es uno de los temas más espinosos cuando se aborda el uso antijurídico de información. La intimidad no sólo está ya amenazada sino realmente invadida por las redes telemáticas. Los Estados, los gobiernos y la justicia han tardado en reaccionar. En principio, al menos

---

11 Juan Luis Cebrián. *Op cit.*

legalmente, los datos de las personas no deberían almacenarse ni usarse sin autorización. Al no existir límites legales en muchos países, y con la capacidad que dan las tecnologías de información de guardar, procesar y transmitir información, la creación de bases de datos, perfiles y todo tipo de información sobre las personas se vuelve prácticamente ilimitada e incontrolable.

Los métodos y prácticas pueden ser tan diversos como los fines que se buscan al penetrar el espacio íntimo mediante la tecnología. Por un lado se encuentra la invasión del espacio virtual personal a través de publicidad basura o de mensajes de correo electrónico no solicitados (*spam*) que abarrotan nuestro buzón, enviados por mercaderes, estafadores, viciosos, o solitarios internautas. Este fenómeno es consecuencia muchas veces de una difusión no autorizada de los datos de correo o direcciones personales de los usuarios de Internet. Toda una industria que recoge, clasifica, engaña a los usuarios con falsas encuestas, ofertas, regalos o con las famosas cadenas de mensajes en apoyo a supuestas campañas comunitarias sirven a empresas y personas para recoger de forma no autorizada la dirección virtual de millones de usuarios, datos que son usados posteriormente con diversos fines.

Otro aspecto estrechamente ligado se produce cuando es invadido no sólo ya el correo (dirección electrónica) sino cuando información sobre la vida de la propia persona se convierte en objeto de uso por parte de terceros. Hasta ahora, los gobiernos reaccionaban solamente en casos protegidos por preceptos tradicionales, tales como el secreto bancario o médico, pero el fenómeno es mucho menos visible en situaciones novedosas o cuando la información personal es usada con fines distintos para lo cual fue obtenida.

Este es el caso, por ejemplo, del tráfico y comercialización de perfiles de consumidores que se hace a través de Internet. Un informe de la Comisión Federal de Comercio de los Estados Unidos señala que el 90% de las páginas o sitios web comerciales obtiene y clasifica datos sobre los usuarios que las visitan, sólo un 14% informa a las autoridades de esta práctica y apenas un 2% tiene políticas de protección de la información personal. La reventa posterior de esta

información en el mercado globalizado es algo que resulta obviamente difícil de descubrir y combatir como no sea con el apoyo de los mismos que la practican.

La mercantilización, el robo y el uso no autorizado de información puede generar consecuencias como la falsificación de identidad para cometer delitos (el equivalente a que nos fuese hurtada la cédula de identidad para ser usada por delincuentes), estafas y fraudes de todo tipo. Pero también la simple difusión de información personal a través de los medios telemáticos afecta el carácter inviolable de la intimidad y la vida personal, lo que en algunos casos se tipifica como la divulgación de secretos personales. La naturaleza «ingobernable» de la red hace que la difusión de tales secretos se convierta en una práctica común contra la que no parece haber hasta ahora legislación, ni experiencia de combate efectiva.

VIOLENCIA, PORNOGRAFÍA Y RACISMO

Una de las más cotidianas y evidentes amenazas que encara la naciente sociedad digital tiene que ver con la difusión de información que lesiona los derechos humanos y los valores fundamentales de la democracia. Las redes de información se expresan así como una ampliación del espacio social real, con sus esperanzas y problemas. La promoción de la violencia, el terrorismo, la pornografía, y el odio racial, entre otros antivalores, encuentran en los medios digitales masivos y propicios canales de expresión, públicos cautivos, y sorprendentes fuentes de financiamiento, que de alguna manera dibujan la miseria espiritual de la sociedad tecnificada.

La difusión de contenidos delictivos constituye sin duda uno de los mayores peligros que enfrentan los ciudadanos en un entorno dominado por las tecnologías de información. Nuevos términos, como la llamada literatura basura (ficción-bite) género de extrema y masiva violencia, aparecen en el escenario y al alcance de cualquiera. Como afirma Don Tapscott, la sordidez y la perversión recorren las alcantarillas

de las autopistas de la información. En particular, la entronización de la pornografía como una de las aplicaciones asesinas[12] de Internet, es decir la abundancia de materiales pornográficos en la red, su descarada comercialización, el surgimiento de toda una industria internacional de pederastia y trata de blancas, constituye tal vez uno de los mayores retos para los gobiernos y ciudadanos en los tiempos por venir. A este respecto, algunas estadísticas señalan que hasta comienzos del año pasado existían más de diez mil sitios (o páginas en Internet) dedicados a la pornografía infantil recibiendo más de diez millones de visitas diarias. Cifras que, por otra parte, revelan el grado de soledad, desamor y pobreza espiritual de la sociedad moderna.

Otra área que ha reclamado la persistente atención de los gobiernos se refiere a la divulgación libre de información violenta o generadora de violencia. El gobierno francés exigió hace un par de años al gobierno norteamericano el cierre de un servidor de Internet, ubicado en San Diego, California, donde se colocaba información sobre la preparación de bombas, pues presumía que dichas instrucciones habían sido usadas en atentados terroristas cometidos en París. Los extremistas y nazis usaron y siguen usando la red para defender sus fanáticos planteamientos y han hecho de Internet una tribuna para glorificar, entre otros, al recientemente ejecutado terrorista Timothy McVeigh, ejecutor del atentado de Oklahoma. Este mismo año un finlandés fue acusado de planear y ejecutar la muerte de su padre, pero además de haber usado un sitio en Internet para divulgar métodos para cometer homicidios, incluido el crimen del que se le acusa. En términos de intolerancia política, fanatismo religioso y violencia terrrorista el espacio virtual demuestra ser un terreno mucho más temible de lo que se piensa.

Otro asunto, que a veces se confunde deliberadamente tiene que ver con las protestas sociales, políticas y de grupos contestatarios, que muchos gobiernos quieren acallar, y que encuentran en la red

---

12 Aplicaciones asesinas o *killer applications*, en inglés, se refiere a una innovación tremendamente exitosa y que liquida de forma violenta a la competencia.

canales de expresión nuevos y poderosos. Hoy es imposible pensar que la lucha de los zapatistas en México y de las mismas FARC en Colombia hayan podido ser conocidas en muchos países si no fuese por su difusión a través de Internet.

Lo mismo puede decirse respecto a ciertos hechos del conflicto de los Balcanes (ex Yugoslavia) donde los diversos grupos en pugna han trasladado hasta las redes digitales sus respectivos conflictos, desatando verdaderas guerras informativas en la red. Recientemente, en pleno auge del choque palestino-israelí, el sitio en Internet de la Cancillería de Israel fue atacado mediante el simple procedimiento de solicitar numerosos accesos simultáneos, es decir, colocar a miles de personas a tratar de ingresar al sitio al mismo tiempo, lo cual hizo que el servidor (computador) que lo hospedaba colapsara.

Iniciativas que buscan imponer un control burocrático de los contenidos se han adoptado por tanto en países de gobiernos totalitarios como China y Cuba, altamente preocupados por la información que pueda salir de sus fronteras. A pesar de ello, la facilidad que brinda Internet para saltarse los controles permite siempre que los intentos de controlar los contenidos sean tan absurdos como vanos.

Pero este fenómeno no ocurre sólo en los países con regímenes no democráticos. En los países democráticos, los gobiernos se debaten hoy en día entre imponer leyes y sanciones a quienes difundan información de carácter delictivo (o que ellos consideren como tales) y de apelar a la colaboración de los privados que pueden mediante un autocontrol, limitar la difusión de este tipo de contenidos.

Por lo general, los Estados, temerosos ante el poder de un medio tecnológico que escapa a su control directo, han optado por la vía fácil de la represión. Con la promulgación de la Ley de Decencia de las Comunicaciones de 1995, el gobierno norteamericano trató de darle una temprana y disuasiva respuesta, imponiendo severos controles de contenidos.

El resultado fue pobremente decepcionante. La Ley, impulsada por el entonces vicepresidente Gore, fue catalogada como un ataque a la libertad de expresión y como un intento del gobierno de regular la

comunicación entre los adultos y fue finalmente declarada inconstitucional por la Suprema Corte. Por lo demás, la Ley Gore se mostró absolutamente ineficiente para reprimir y disuadir. Como afirma John Gilmore, uno de los pioneros de Internet, ésta «interpreta todo intento de censura como un perjuicio y la esquiva». Al menos en esta etapa la censura no parece ser una respuesta eficaz en la red, aunque su promoción como supuesto remedio a la difusión de contenidos delictivos o delictuosos, sí parece seguir siendo un objetivo políticamente atractivo para los gobiernos.

En el fondo, el asunto sobre la calidad democrática y el contenido de la información que circula por la redes de información suscita, un acalorado debate entre quienes ven a Internet como un medio de expresión perfecta, ingobernable e incensurable, y quienes promueven el control de los contenidos en nombre de las libertades civiles y democráticas. De lado y lado se hallan posiciones honestas y cínicas y es eso tal vez lo que impide un consenso razonable sobre este espinoso tema.

El Informe del Club de Roma de 1998, recomendaba no caer en uno de los extremos. Los peligros, afirmaba, vienen de ambas partes. Por un lado la censura gubernamental, coercitiva y antilibertaria. Por el otro, el supuesto libre flujo de información, ingobernable y manipulable. Ambos extremos llevarían a un fracaso permanente y niegan de plano la posibilidad de un consenso social, abierto y transparente que permita coexistir la libertad y responsabilidad. Debería comenzarse, recomendaba el Informe, por impedir mediante todas las formas legales posibles el anonimato a fin de poder exigir responsabilidades concretas y personales a quienes atenten contra la libertad ajena, usando abusivamente la propia.

Esto es vital porque la información que promueva la violencia, la destrucción de los valores democráticos, el odio entre los seres humanos y los pueblos, es considerado en nuestra legislación como un atentado mismo a nuestros valores como nación. Más allá del debate sobre censura y control, debate por lo demás teñido de los intereses en pugna, sean éstos personales, políticos o económicos, la verdad es que las redes de información se encuentran hoy en buena medida

abarrotadas de contenidos violentos. Ese es un reto que toda sociedad democrática debe afrontar de un modo sincero y razonable.

SEGURIDAD Y DEFENSA: LA GUERRA DESDE EL CIBERESPACIO

El tema de la seguridad del Estado y de los secretos militares constituye hoy también un tema de acalorado debate. Es sabido que durante la Guerra del Golfo, en 1991, cuando Internet estaba en pañales, el ejército norteamericano experimentó con ejercicios de desinformación mediante redes informativas para confundir al estado mayor iraquí. Desde entonces, los juegos de guerra y las estrategias militares deben contar con los ataques desde el ciberespacio en caso de conflictos militares.

Pero si pueden hacerlo los gobiernos y sus estructuras militares, hoy también los ciudadanos y privados, pueden desarrollar su particular guerrilla informática. El acceso mediante medios telemáticos a las bases de datos de los Estados y gobiernos constituye en la actualidad una práctica entre expertos informáticos, más común y posible de lo que se cree. No se trata ya de un asunto de ficción, como lo anunciaron películas hace 10 ó 20 años.

La realidad es que los Estados y gobiernos deben automatizarse para conectarse a la nueva economía global y aprovechar las ventajas de interacción, eficiencia y participación que brindan las nuevas herramientas tecnológicas. Este es el punto de partida de quienes proponen un modelo de gobierno electrónico, es decir, un esquema donde el Estado traslada buena parte de su información, servicios y relaciones con la sociedad a las plataformas digitales. Sin embargo, la posibilidad real de que los servicios públicos puedan ser saboteados a distancia, de que las bases de datos sean intervenidas y de que muchos de los secretos de Estado sean divulgados afectando las relaciones internacionales, y creando un caos impredecible, constituye un tema de preocupación en predios del sector público de todo el mundo.

A este respecto, además de legislar, los gobiernos han venido creando nuevas instituciones que tratan de responder al reto creciente de mantener la autoridad del Estado en un medio que luce ingobernable. Alemania, por ejemplo, fue el primer país que creó una policía del ciberespacio, dedicada exclusivamente a perseguir la pornografía y la violencia. Intentos como éste, burlados a veces por la extraterritorialidad de los medios digitales, evocan la necesidad de acuerdos internacionales más amplios y completos para crear una cultura de defensa de lo público en las redes telemáticas.

Ya sabemos que el camino más fácil es tal vez el menos efectivo y deseable, como lo es la simple represión. El Estado democrático debe replantearse nuevamente su rol en el nuevo contexto digital, o dicho en palabras de Juan Luis Cebrián «averiguar qué papel tienen los Estados nacionales ante un fenómeno global que, por lo demás, es gobernado progresivamente por un sistema de corporaciones económicas y que no responde a los cánones clásicos de la autoridad política».

MANIPULACIÓN DE CAJEROS AUTOMÁTICOS Y CLONACIÓN DE TARJETAS

Esta modalidad delictiva es una de las más difundidas y con mayor variedad de fórmulas. Se manifiesta desde el simple robo de tarjetas magnéticas y claves de acceso, hechas por una persona actuando mediante trucos y sencillos engaños a los usuarios, hasta la defraudación masiva a través de asociaciones delictivas que involucran no pocas veces a empleados bancarios, pasando por el uso de sofisticados sistemas de clonación de tarjetas mediante la copia y reproducción digital de la información contenida en las bandas magnéticas.

Aunque parezca un delito de poca monta en relación con los fraudes cometidos contra bancos y grandes corporaciones, la verdad es que se trata de un ataque directo contra los ciudadanos cuyos montos agregados supone un elevado costo económico y social. Por esta razón,

las autoridades no deben descuidar su prevención y combate. Ya sea que se cometa individualmente o mediante redes del delito organizado, la manipulación de dispositivos electrónicos con fines delictivos debe ser atacado por el Estado como un problema de primer orden.

PIRATERÍA DE SOFTWARE Y ROBO DE INFORMACIÓN

El método más común en el hurto de software es el de la copia de los archivos de datos (*data files)* y su reproducción con fines mercantiles, de apropiación u otros. En el segmento de los programas de gran uso y mercado (sistemas operativos populares, paquetes de oficina, etc), la copia es un método usual y rápido. En el área de programas especializados y no masivos (software hecho a la medida), la copia se realiza mediante programas especialmente creados para tal fin, usando la técnica de *superzap* o mediante la introducción de rutinas tipo «Caballo de Troya».

La violación de los derechos de autor y la piratería del conocimiento constituyen un rentable negocio para quienes actúan al margen de la ley. Los principales afectados son por supuesto los autores y empresas productoras del software quienes dedican años y recursos a la investigación y desarrollo de nuevos productos que pueden ser copiados y usados por cualquiera en su propia casa, gracias a la versatilidad del formato digital.

Detrás se encuentran no sólo hackers y otros genios de la red que se proponen desencriptar los códigos de seguridad de los programas sino incluso grandes empresas que se dedican a tratar de robar el conocimiento desarrollado por otros. Los beneficiarios en este caso no son sólo las empresas piratas sino los usuarios que pueden acceder a software y otros productos digitales de primera mano a precios de gallina flaca. Es común en cualquier parte del mundo ver cómo en las calles se comercializan a precios realmente populares productos y software de última generación. Un software que puede costar entre 500 y 600 US $

en su licencia original, puede conseguirse en cualquier calle del centro de Caracas o Maracay entre 8 mil y 15 mil bolívares, y a veces menos.

Este fenómeno tiende a incrementarse debido al desplazamiento creciente de una parte de las compras de software y otros bienes de conocimiento hacia Internet. De hecho, en Estados Unidos se estima que en los próximos cinco años, dos de cada tres ventas internas de software, y tres de cada cinco ventas hacia el extranjero se harán por Internet[13]. La Business Software Alliance calcula que más de 40 mil millones de dólares al año se pierden por este concepto, sin incluir los ingresos que dejan de percibir los Estados en materia de impuestos.

Obviamente, se trata de un tema espinoso y sobre el que no hay un acuerdo general. Nuevamente las peculiares características de lo digital facilitan la copia y reproducción de la información, su masiva difusión y transformación por parte de los usuarios. Las primeras y grandes batallas judiciales se han librado alrededor del tema de la copia ilegal de software y de la reproducción e intercambio de archivos musicales en formato digital (mp3) a través de Internet, esto último a raíz del polémico caso Napster[14]. Las grandes empresas productoras y agentes comerciales han librado una guerra a empresas de Internet y movimientos espontáneos que digitalizan conocimientos y bienes como la música y lo ofrecen de forma gratuita. Esta batalla apenas comienza y está lejos de decidirse porque, amén de la comprensible defensa de los derechos de autor, se encuentra todo un negocio de intermediación que encarece los bienes culturales. La red, aquí nuevamente actúa como un factor de perturbación, casi

---

13 Business Software Alliance (BSA). *Critical High Tech Issues for 2001-2002. Summary*. Fuente: www.bsa.org.

14 Después de una larga y polémica batalla judicial, la empresa Napster.com ha sido obligada por un juez federal norteamericano a tener que filtrar los archivos ofrecidos a través de su sitio en Internet y a tener que cobrar por este servicio, antes totalmente gratuito. Los puntales empresariales en esta guerra han sido algunos de los grupos de rock más famosos, como Metallica, y sus representates comerciales en alianza con las productoras y distribuidoras a nivel mundial. Lo curioso de este caso es que mientras en sus canciones algunos grupos de rock denuncian la miseria del mercantilismo y el consumismo, en el terreno real la protección de sus beneficios los lleva hasta los juzgados para defender ese mismo sistema.

de subversión para los propios intereses mercantiles, muchas veces monopolizados u oligopolizados.

En materia de robo de información, y específicamente en el caso de los sistemas de telecomunicaciones y redes de información remota, la práctica delictiva clásica consiste en la introducción en los centros de datos con el fin de acceder a información no autorizada. La intercepción técnica de contraseñas y claves y la escucha telefónica (pinchar la línea) es también un frecuente modus operandi. Contrariamente a lo que mucha gente piensa, la instalación de escuchas telefónicas (introducción en celulares y otros dispositivos móviles) con el fin de obtener contraseñas e información, es técnicamente mucho más confiable y peligrosa en el caso de los sistemas de telecomunicaciones y teleprocesos que en el caso de la comunicación oral, y se espera que en el futuro constituya un medio de uso delictivo frecuente. La comunicación interpersonal nunca estuvo más expuesta y nunca estuvo más en peligro de ser incautada por otros que ahora cuando, paradójicamente, disponemos de una libertad casi ilimitada para comunicarnos.

FRAUDE MEDIANTE LA MANIPULACIÓN POR COMPUTADORES O MANIPULACIONES DE PROGRAMAS

Sucede cuando se produce una transformación o alteración de los programas existentes de una organización mediante:

a.- El uso de recursos de programación como el Caballo de Troya o la introducción de virus informáticos.
b.- A través de la introducción de programas autónomos creados con el fin de producir dicha alteración.
c.- Mediante el uso de programas especiales capaces de eludir los mecanismos de seguridad del programa original (tales como el *superzap*).

El fin puede ser diverso: alterar bases de datos para desviar recursos financieros de la organización hacia cuentas externas, ocultar operaciones ilícitas realizadas en la organización, eliminar deudas o crear saldos inexistentes en cuentas personales, destruir bases de datos y sistemas de información, etc.

SABOTAJE POR ORDENADOR

Se distinguen en este delito dos métodos: aquellos que causan daño físico y aquellos que producen daño en el sistema lógico. Algunas revistas *underground*[15] tanto en Europa como en Estados Unidos recomiendan a los usuarios, generalmente en casos de conflictos laborales con una empresa, técnicas de destrucción física tales como: introducción de papel esmerilado encima de las partes electrónicas leíbles de una tarjeta con el fin de destruir los lectores de símbolos, insertar hierro cortante, clips o pequeños trozos de hojas de aluminio en los mecanismos y ranuras de los ordenadores (unidades de CD, diskette, DVD, etc) con el fin de causar cortocircuitos, verter café, soluciones con sal o sustancias cáusticas de limpieza sobre los teclados y partes de los equipos, arrojar humo, spray u otros gases dentro del computador, provocar temperaturas extremas calentando partes del computador con cigarrillos o saboteando los sistemas de aire acondicionado, interferir las instalaciones eléctricas, hasta colocar ratones (reales) en las oficinas para que roan los cables y equipos[16].

El método más popular de causar daños al sistema lógico es a través de programas destructores (*crash programs*) que pueden borrar grandes volúmenes de datos en un período relativamente corto. Es un delito muy difícil de probar porque el programa destructor puede dejarse instalado en un sistema para que se active después que su autor haya

---

15 Revistas de orientación de izquierda, intelectuales y críticas del sistema de mercado que circulan fuera de los círculo comerciales.

16 Citado por Ulrich Sieber.

desaparecido o no pueda ser relacionado con el daño, o porque muchas veces el daño es imperceptible, como en los programas o virus que producen la lentitud de los sistemas pero no los dañan. Una de las modalidades más usadas son los llamados programas cáncer, rutinas sencillas que se autorreproducen y que pueden llegar a dañar a todos los sistemas y unidades conectados al sistema infectado inicialmente.

Por supuesto, cada delito debe ser clasificado de acuerdo al peligro de su uso criminal y de las consecuencias que genera. Sin embargo, la clasificación de estas conductas y hechos como delitos resulta importante dado que muchas veces las víctimas del sabotaje por computadora no están familiarizados con estas técnicas y por lo general sufren pérdidas adicionales debido a su incapacidad para identificar estas técnicas como actos deliberados de sabotaje. Por el contrario, buscan durante mucho tiempo los defectos en sus sistemas dando así más tiempo al delincuente para continuar con su actividad criminal.

EL COMPUTADOR COMO HERRAMIENTA PARA COMETER DELITOS ECONÓMICOS TRADICIONALES

En los últimos años, a la sombra de la publicidad y de la atención de la prensa que han atraído sobre sí los piratas (hackers) y la difusión de virus a través de las redes telemáticas, se ha incrementado el uso de los computadores y de los medios informáticos en general para cometer delitos económicos corrientes a expensas, o bien de los socios o dueños de empresas, de los consumidores, de inversionistas o de los gobiernos. La mayoría de los casos descubiertos se refieren a la manipulación de las cuentas, ingresos, balances, inventarios y declaraciones de impuestos. Un mecanismo frecuentemente usado consiste en borrar las listas de stock (inventarios) y los balances para ocultar la comisión de delitos económicos, así como la modificación de los sistemas contables para subfacturar o sobrefacturar de acuerdo a determinados objetivos fiscales.

El uso de computadoras para cometer delitos económicos tradi-

cionales se ha hecho especialmente claro en delitos como la falsificación de cheques y el lavado o legitimación de capitales provenientes del narcotráfico, debido a la facilidad con que los sistemas digitales permiten simular la realización de operaciones aparentemente legales o permiten ocultar la comisión de determinados delitos.

Delitos informáticos en Venezuela: un problema de Estado

Venezuela constituye hoy en América Latina uno de los paraísos para la comisión de todo tipo de delitos informáticos. La ausencia de un marco legal que atienda el fenómeno, la debilidad institucional de las policías, la Fiscalía y los tribunales, la falta de un adecuado control tanto por parte del Estado como de los bancos y otras empresas de servicios, así como la ausencia de una cultura teleinformática que permita a ciudadanos y autoridades comprender y actuar con efectividad, hacen que nuestro país sufra toda suerte de ataques delictivos perpetrados mediante el uso y manipulación de medios electrónicos.

Hay que reconocer que, tal como sucede en ciertos casos de enfrentamientos con delincuentes comunes, donde los transgresores de la ley se hallan mejor armados y preparados que los policías, en el medio teleinformático los delincuentes llevan hoy la delantera. Desde el simple robo físico de tarjetas o claves de tarjetas de débito, operación muchas veces realizada en complicidad con empleados bancarios, la clonación o falsificación de tarjetas de crédito, la violación de derechos de autor mediante la copia ilegal de software, música y otros bienes culturales, la venta de información personal sin autorización en Internet, la intercepción de comunicaciones privadas, la publicidad engañosa, entre otros, constituyen hechos cotidianos frente a los cuales los usuarios de los medios telemáticos se encuentran desprotegidos, el Estado no tiene capacidad de respuesta y las empresas se mueven en la indefinición.

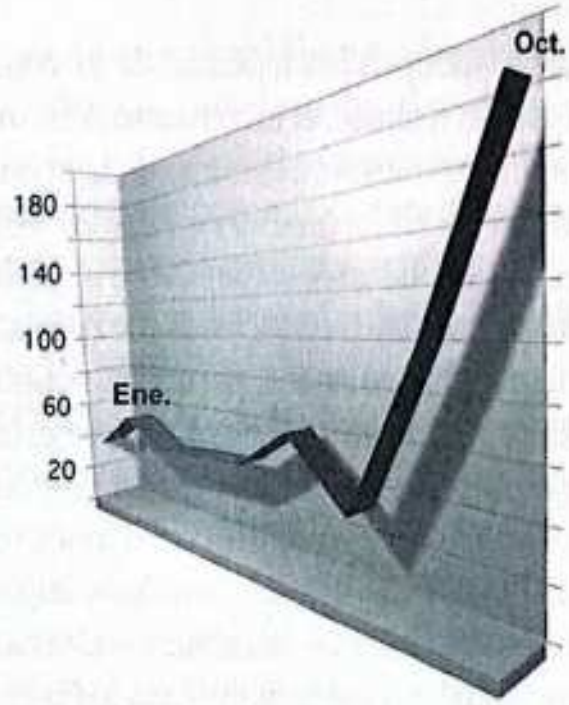
De hecho, la propia Superintendencia de Bancos y otras instituciones financieras (Sudeban), el organismo responsable de la fiscalización del sistema financiero, este último uno de los blancos preferidos

de los delincuentes informáticos, reconoció ante la Asamblea Nacional el preocupante incremento del número de fraudes electrónicos en Venezuela durante los últimos años. Sudeban atribuye este fenómeno a que el conocimiento de los que llevan a cabo este tipo de actividad ilícita avanza más rápido que la materia legislativa y las herramientas de control. Pero, como se sabe, la ineficacia o el atraso no es sólo de las leyes, sino también de los organismos que están encargados de perseguir este tipo de delito, o de velar por el cumplimiento de las leyes actuales.

Este rezago de la sociedad frente a la tecnología aplicada al delito, se refleja en los altos grados de desinformación, falta de conciencia acerca del problema por parte de muchos usuarios de estos medios y la carencia de estadísticas claras que reflejen lo que está sucediendo. Se ha empezado a actuar bajo la presión de una realidad compleja y novedosa sin que se cuente con adecuados instrumentos para afrontar científicamente el problema.

En la Policía Técnica Judicial, por ejemplo, a través de la División contra la Delincuencia Organizada, se creó hace poco más de un año una brigada integrada apenas por cuatro funcionarios que atiende los casos de delitos informáticos. Como lo expresó a la Comisión de la Asamblea Nacional, el propio Comisario Luis Guanda Araujo, este equipo humano es absolutamente insuficiente, aunque, pese a las limitaciones, dicha brigada ha logrado capturar a algunos delincuentes y decomisar equipos a través de los cuales clonan las tarjetas de crédito y débito.

El auge de los delitos informáticos es por tanto un hecho que ya no se puede ni se debe ignorar. Sólo en un área como lo es el fraude mediante tarjetas de crédido y de débito, el Instituto de Defensa y Educación del Consumidor (Indecu) recibió en el año 2000 más de 600 denuncias, mientras sólo hasta febrero de este año han sido reportadas casi 300 denuncias (ver gráfico siguiente).



DELITOS INFORMATICOS DENUNCIADOS A LOS BANCOS
AÑO 2000

Casos Año 2000	618
Casos Ene-Feb. 2001-05-31	295
Bancos e Inst. financieras afectadas	22

Obviamente, estas cifras[1] no recogen fielmente la magnitud del problema debido al desconocimiento del público y a la falta de estructuras técnicas que den soporte científico a la investigación policial. De hecho, la PTJ ofreció recientemente a los medios de comunicación una cifra escalofriante. Según la policía científica del país sólo en el año 2001, el monto defraudado por las redes de clonación de tarjetas supera a estas alturas los 3 millardos de bolívares[2].

---

1 Fuente: Indecu. Las cifras entre los diversos organismos involucrados suelen no coincidir, dados precisamente los problemas de desinformación y falta de educación en los usuarios. Pese a este hecho, la tendencia entre las cifras aportadas por PTJ y el Indecu reflejan el mismo sostenido crecimiento de los delitos informáticos.

2 El Comisario Luis Guanda, jefe de la División contra la Delincuencia Organizada del CTPJ declaraba a los medios recientemente que: «Hay un número incontable de estafas y fraudes electrónicos que no se presentan ante la PTJ y que sólo conocen las instituciones bancarias. Seguramente, la dimensión de este negocio es mayor de lo que podríamos imaginar...» ,*El Nacional.* Siete días. 27 de mayo de 2001.

Sin embargo, independientemente de la relación entre las diversas estadísticas y la realidad, el incremento del número de denuncias hacia los dos pimeros meses de este año demuestra que los delitos informáticos constituyen un fenómeno de auge en Venezuela.

En la tarea de cuantificar y actuar sobre el problema, organismos como el Indecu desde hace año y medio se han sumado a la tarea de enfrentar los fraudes informáticos, particularmente de los usuarios de tarjetas de crédito y de débito. El organismo, cuya función consiste en apoyar los reclamos de los consumidores y lograr la devolución del dinero defraudado, estima que en este lapso, el monto de pérdidas por fraudes mediante medios de pago electrónicos, superó los mil 300 millones de bolívares, sin contar los casos que los usuarios no denuncian al Indecu sino que tramitan directamente con los bancos.

Estos hechos y cifras nos prueban que estamos frente a un problema social, que no sólo afecta a usuarios de forma individual sino que afecta el patrimonio de miles de venezolanos y altera, entre otros, el funcionamiento del sistema financiero, produciendo pérdidas a las empresas y daños a la economía del país. Eso es aún más grave si se considera que la tendencia en el mundo es a sustituir los medios de pago basados en papel u otros soportes físicos (billetes, cheques, monedas) por medios de pago electrónicos.

Mientras los delincuentes refinan y actualizan los mecanismos de la delincuencia tecnológica, en Venezuela actualmente no existe una política de Estado que integre los esfuerzos de todos los actores involucrados en el problema. A la debilidad institucional del Ejecutivo y el Poder Judicial, se le suma una cierta desorganización por parte del sector privado, que ha actuado igualmente presionado bajo la realidad de la penetración delictiva de sus sistemas, pero sin contar hasta ahora con un cuerpo de acciones hacia la comunidad que permita una acción en conjunto.

De hecho, el propio representante de la Asociación Bancaria, Juan Carlos Escotet, reconoció ante la Comisión Investigadora de la Asamblea Nacional, que la banca se encontraba hasta el año pasado en un proceso de «recabar información» a fin de modificar normas y

establecer mecanismos de seguridad que fuesen luego sometidas a la aprobación de todos los miembros del sistema financiero privado, para su puesta en ejecución de forma coordinada. Mientras los bancos se ponen de acuerdo para prevenir en forma conjunta estos delitos, sus propios cálculos sitúan las pérdidas mediante fraudes y estafas con medios electrónicos en el orden de 7 millardos de bolívares sólo en el primer semestre del 2000.

En privado, voceros de la banca reconocen que la penetración interna de sus sistemas informáticos, posible gracias a la complicidad interna, es la causa fundamental del incremento de fraudes y estafas en tarjetas de débito y de crédito, lo que hace pensar que dichos delitos se realizan mediante la conjunción de personas y grupos organizados para tal fin, es decir, delincuencia organizada. Esta aseveración coincide con los informes de PTJ y la percepción del mismo Indecu, quienes afirman que muchas tarjetas son falsificadas y clonadas, aún antes de llegar a sus destinatarios, es decir, dentro de la propia estructura de los bancos e instituciones financieras.

Existe, por supuesto, más allá de los fraudes a las tarjetas electrónicas, una amplia gama de delitos cometidos a través de medios telemáticos que se practican en Venezuela. Delitos que producen cuantiosos daños, y que sin embargo, no gozan de la misma proyección o interés público. El robo, o copia ilegal de software, datos, música y otros bienes culturales, posible, gracias a la manipulación de la tecnología digital constituye, por ejemplo, un problema que afecta la credibilidad de Venezuela en el ámbito del comercio internacional. La Bussines Software Alliance, un organismo internacional privado dedicado a descubrir y denunciar el robo de este tipo de productos intelectuales estima que más del 62% del software que se utiliza en Venezuela es pirata, es decir, ha sido copiado y es usado de forma ilícita sin pagar a los dueños por las licencias y patentes. Sólo en 1999 las pérdidas para la casas y empresas productoras de software se estimaron en 63 millardos de bolívares por concepto de piratería[3].

---

3 Aunque por su magnitud económica y extendida aparición, delitos como la violación

La falta de una legislación efectiva y la imagen de que nuestro país es terreno fértil para la piratería de obras, productos intelectuales y bienes culturales daña las posibilidades de inserción de Venezuela en el contexto de los actuales acuerdos comerciales internacionales, una de cuyas bases es el respeto a los derechos de autor y la protección al conocimiento.

La magnitud que está alcanzando el problema de los delitos informáticos en Venezuela, debe necesariamente llamar a la reflexión al Estado y a la sociedad venezolana en su conjunto. Desde el nuevo Poder Legislativo, representado en la Asamblea Nacional, se inició la tarea de investigar y diseñar las bases de una actualización del marco legal de nuestro país en materia de delitos informáticos. En septiembre del año 2000 se creó la Subcomisión de Delitos Informáticos, dependiente de la Comisión de Finanzas, integrada por los diputados Carlos Tablante, Guillermo Palacios, Elías Matta, Héctor Vargas y Norberto Peña.

La Comisión se ha dedicado a recoger información, intercambiar opiniones y criterios con diversos actores del medio, conocer los esfuerzos que desde el sector público y privado se están haciendo para enfrentar el fenómeno y proponer, a partir de este diagnóstico, un conjunto de medidas legislativas que puedan ser parte de una nueva política del Estado venezolano frente al delito informático.

La tarea se ha centrado en estimular el interés por este fenómeno, llamando la atención sobre la realidad actual, las debilidades que presenta la sociedad venezolana y la integración de esfuerzos a fin de enfrentar con seriedad y visión del Estado este delicado problema so-

---

de los derechos de autor, piratería de software y otros asociados al uso y reproducción ilegal de conocimiento constituyen un problema de primer orden en Venezuela, la investigación y las fuentes consultadas se centraron en los delitos de orden financiero, por lo cual se requeriría una investigación mucho más amplia de estas modalidades delictivas en nuestro país. Es de destacar que en Venezuela existe tanto la Ley sobre Derecho de Autor como la Decisión 351 de la Comisión del Acuerdo de Cartagena, adoptada por Venezuela, que forman el marco regulatorio en este sector. La propuesta de ley que presenta este libro categoriza sin embargo todas las modalidades delictivas susceptibles de ser cometidas mediante el uso o través de medios informáticos y teleinformáticos.

cial. El fin, sumar el trabajo del Ejecutivo, el órgano legislativo, el Poder Juidicial, las empresas y los mismos usuarios de los medios telemáticos, a fin de fortalecer una cultura de seguridad y prevención que combata este tipo de delitos.

CLONACIÓN DE TARJETAS: EL FRAUDE ELECTRÓNICO

Recientemente, la prensa venezolana daba cuenta de la clonación de la tarjeta de crédito del presidente del Banco Central de Venezuela, es decir, nada más y nada menos que de la cabeza ejecutiva más alta de la institución rectora de las finanzas en nuestro país. Hay que imaginarse qué sensación debe haber recorrido a los millones de tarjetahabientes venezolanos al enterarse de que el jefe máximo del instituto de finanzas más importante del país, podía también ser víctima de una clonación, como lo son a diario miles de nuestros ciudadanos que han confiado en el sistema financiero y en las leyes venezolanas en el uso de tales instrumentos económicos.

Sin duda el delito informático más extendido, frecuente y notorio de cuantos se cometen hoy en día en Venezuela consiste en la falsificación y/o clonación de medios de pago electrónico, es decir, tarjetas de crédito y de débito. Es un delito que consigue un ambiente propicio dadas las necesidades y tendencias en el sistema financiero a sustituir los medios de pago tradicionales por medios electrónicos debido a menores costos y mayor eficiencia, y estimulado por los rezagos tecnológicos de los órganos públicos como policías, fiscales y jueces, que impiden una cabal comprensión y combate a estos delitos.

La clonación de tarjetas ilustra claramente la articulación de mecanismos delictivos tradicionales con el uso de poderosas tecnologías digitales y hace pensar que se trata, más que de delitos cometidos en solitario, de la actuación de poderosas redes de delincuencia organizada.

El modus operandi es extremadamente sencillo. Mediante el

uso de lectoras ópticas o «pescadoras»[4], instaladas en comercios legales, se logra capturar de forma subrepticia la información del dueño de la tarjeta grabada en la banda magnética de ésta, al momento en que el cliente la entrega para el pago. Es un mecanismo simple, rápido y que opera incluso ante la vista de las propias víctimas, quienes ignoran que mientras su tarjeta es solicitada para confirmar la validez, al mismo tiempo es sometida a un proceso que «captura» en este dispositivo la información que servirá para clonar la tarjeta.

Cada pescadora puede almacenar hasta 99 datos de tarjetas y se estima que por cada dato de banda magnética pescada, el «pescador» obtiene entre 30 y 50 mil bolívares, lo cual significa que por cada pescadora llena de datos robados subrepticiamente, puede obtenerse de forma relativamente segura hasta 4 millones 950 mil bolívares. La comparación de rentabilidad con los delitos tradicionales muestra aquí con todo dramatismo, cómo la manipulación de medios informáticos amplía su potencial en manos delictivas.

Una vez que se han grabado las informaciones de las tarjetas, la pescadora es llevada a un sitio donde se encuentra el resto del equipamiento: una magnetizadora, un quemador de CD[5], una minicomputadora, y equipos para impresión del plástico (la tarjeta), todo lo cual tiene un costo aproximado de 8 millones de bolívares. Usando un software diseñado para ello, la información pescada de las tarjetas es transferida mediante la magnetizadora a una tarjeta virgen, la cual, por supuesto, ya tiene la información del tarjetahabiente, y bien sea con la complicidad de las personas que trabajan en ciertos establecimientos, se hacen diferentes operaciones, que son las que afectan al tarjetahabiente y finalmente a las instituciones bancarias (ver infografía *Clonación de tarjetas* en la página siguiente).

---

4 Las «pescadoras» son dispositivos de aproximadamente diez centímetros de longitud, con una abertura y una batería pequeña, que pueden ser llevadas en un bolsillo por el mesonero de un restaurant o el vendedor de una tienda. El principio de funcionamiento es similar al de los escáner de escritorio que pueden capturar imágenes o textos y convertirlos en información digital.

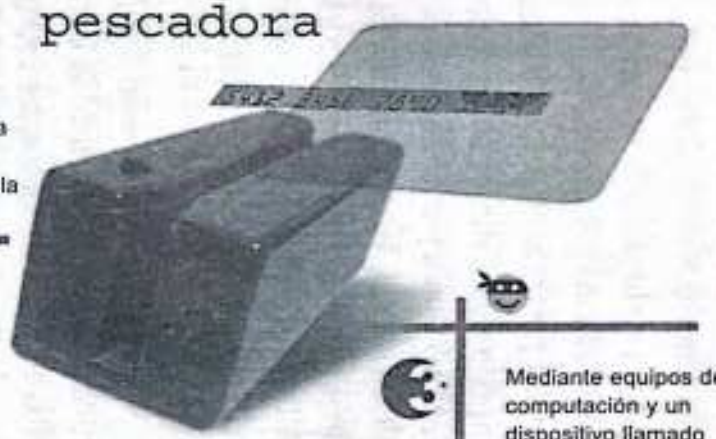
5 Un quemador de CD (*cd writer*) es un aparato que permite reproducir digitalmente, copiar y almacenar información en discos compactos (CD).

Clonación de tarjetas: una red delictiva

1. El tarjetahabiente entrega su tarjeta para pagar en un local comercial. El vendedor, mesonero o dueño puede ser parte de la red delictiva que realiza la operación.

2. Al momento de la verificación, la tarjeta original es "pasada" por la pescadora la cual almacena los códigos de la cuenta

pescadora



3. Mediante equipos de computación y un dispositivo llamado "magnetizadora" se logra grabar la información pescada en una tarjeta virgen

4. La tarjeta clonada sale a la calle, donde es vendida o usada para compras, pagos, transferencias de fondos, muchas veces con complicidad de locales comerciales. En otras ocasiones, esta vez con conexiones en los bancos, la tarjeta es clonada incluso antes de que llegue a manos del tarjetahabiente.

5. Los pagos al "pescador" por una pescadora full de códigos (100 tarjetas) puede estar entre los 40 y 50 mil Bs. El fraude total en Venezuela sólo en el año 2001 se calcula en más de 3 millardos de Bs.

Es de destacar que para utilizar la pescadora no se necesitan conocimientos técnicos especiales, lo cual facilita la diseminación de los «pescadores» de tarjetas en comercios de todo el país. El saber informático se requiere en la etapa de producción de las tarjetas clonadas debido a la necesidad de manejo de ciertos programas y equipos, software y hardware específicos. Por su parte, los equipos utilizados para la clonación de tarjetas son adquiridos en el exterior a un precio bastante módico, por personas que se dedican única y exclusivamente a trasladarlos desde los Estados Unidos hasta Venezuela. Dada la fácil comercialización de este tipo de equipos en el exterior, la PTJ sugirió una coordinación con el FBI e Interpol para acceder a información sobre este tipo de operaciones comerciales, a fin de detectar compradores, medios usados, frecuencia, etc.

La idea de que se trata de una red delictiva lo demuestra el hecho de que existe todo un proceso que comienza en la importación o introducción ilícita al país de los equipos de clonación, su ubicación en determinados círculos y comercios, la operación técnica y finalmente la comisión de fraude mediante tarjetas clonadas. Se trata de operaciones y actividades diferentes, realizadas por individuos y grupos diferentes pero conectados en una misma red delictiva.

En este caso particular se hace urgente la adopción de acciones concertadas desde el Estado con las empresas franquiciantes, los bancos, el sector comercial y los usuarios para poder enfrentar este novedoso, lucrativo y fraudulento negocio.

EMPLEADOS INFIELES, COMERCIANTES BANDIDOS, USUARIOS INCONSCIENTES

Es importante acotar que la clonación de tarjetas de crédito no sólo se realiza de forma directa en los locales comerciales, sino también a través de la intercepción de las tarjetas que son enviadas a través del correo. Esta operación se realiza conjuntamente con son empleados de estas instituciones públicas o privadas. Cuando se logra la inter-

cepción, la tarjeta se extrae del sobre que debe ser entregado al tarjetahabiente, y con esa información es fácilmente clonada. Cuando al usuario le llega su estado de cuenta, se percata de que la tarjeta fue utilizada.

Tal como ha ocurrido en el resto del mundo, donde cerca del 40% de las estafas y fraudes provienen de infiltraciones o traiciones internas a las propias organizaciones, en Venezuela, la infidelidad de empleados bancarios constituye una fuente o soporte frecuente de muchos delitos. Desde la simple manipulación mecánica de cajeros automáticos para robar tarjetas, la intercepción de tarjetas o el acceso a datos que luego son vendidos a terceros, la debilidad de muchos bancos proviene precisamente de su incapacidad para detectar la complicidad interna.

En ese sentido se refleja una contradicción, pues a pesar de que la banca ha agilizado las operaciones financieras, no se dispone de recursos humanos propios en estas instituciones, que garanticen total y absoluta confianza.

La infidelidad de sus empleados como elementos de los delitos informáticos ha sido reconocido por la misma banca aunque quizá no en la dimensión que se maneja públicamente, y es precisamente el elemento que ha permitido detectar el por qué unos bancos han estado expuestos con mucha mayor frecuencia que otros a actividades ilícitas[6].

---

6 El presidente del Banco de Venezuela, uno de los más afectados por la clonación, informó al Indecu en el año 2000 que tales delitos le costaron al banco un promedio de 12 mil millones de bolívares, por el hecho de tener que compensar o devolverle el dinero a la mayoría de los usuarios afectados. Efectivamente, como lo informó a la Asamblea Nacional, el Indecu constató que hasta el mes de agosto del 2000, el 70% de las reclamaciones de los ciudadanos eran satisfechas. «Hasta ese mes, la situación en el Banco de Venezuela era muy desfavorable; en la reunión que sostuvo el Indecu con el Presidente de dicho banco, éste dio una primera información donde expresó que la razón de tales circunstancias era que ellos tenían el mayor número de tarjetahabientes, y que, por supuesto, el universo era de mayor cantidad al de otros bancos. Sin embargo, el Indecu estuvo estudiando las proporciones, y era desproporcionado el número de tarjetahabientes con relación a los casos afectados, lo que demostraba que las fallas estaban en los sistemas de seguridad del propio banco, argumento que aceptaron los representantes del mismo. Ante tal escenario, en el mes de agosto, fue cambiado todo el sistema con el que funcionaba el banco, e informaron que habían comprado en Israel un nuevo sistema de seguridad el cual iban a poner en práctica». (Declaración del Presidente del Indecu, Samuel Ruh Ríos ante la Subcomisión de Delitos Informáticos de la Asamblea Nacional, año 2000).

La inversión en sistemas de seguridad sólo será eficiente en la medida en que quienes administren y tengan acceso a las bases de datos que manejan dichos sistemas operen con rectitud. Se trata de un aspecto del problema donde las organizaciones financieras pueden aportar mucho, elevando significativamente sus controles internos, y la capacitación y formación ética de su personal.

Otro factor clave en la proliferación de la clonación de tarjetas lo es sin duda la participación, ya no sólo de empleados de bancos y comercios en el proceso de captura o robo de información, sino incluso de dueños de entidades comerciales que, debido a la alta rentabilidad del negocio, se prestan para defraudar a sus clientes, especialmente si se trata de personas pudientes o extranjeros. La vinculación de empresarios a este red delictiva hace aún más difícil a veces detectar la comisión de delitos por la facilidad que tienen de encubrir sus operaciones ilícitas. Ya no es sólo un problema de supervisión de los comercios sino de descubrir hasta qué punto los dueños o encargados también han sido «comprados» para participar en los fraudes mediante clonación de tarjetas. La Asociación Bancaria considera que en los últimos meses del 2000 hubo un desplazamiento de estas bandas delicitivas desde la estructura interna de los bancos hacia los comercios, por la facilidad de operación y multiplicidad de opciones que brindan pequeños y grandes negocios.

En México, donde este problema se ha detectado con fuerza, la Asociación Bancaria de dicho país acordó que cualquier comercio que resulte incurso en una práctica de esta naturaleza, sea expulsado, de por vida, de la posibilidad de obtener franquicia, o sea, licencia para aceptar cualquier tipo de medio de pago de cualquiera de las grandes franquiciadoras de tarjetas (Visa, Master Card, American Express, Dinners). Incluso si alguno de esos establecimientos excluidos de utilizar ese tipo de medio, es contactado por algún banco que decida desconocer el acuerdo y le mantenga el punto de venta, la franquicia a escala internacional le suspende la franquicia al banco. Este tipo de medida sin duda podría funcionar en nuestro país como un estímulo para que los dueños de negocios prevengan la penetración de su

Cómo Reconocer una Tarjeta Válida

No devuelva la tarjeta hasta completar la transacción y siga estos sencillos pasos:

Compare los números de las tarjetas

El número de la tarjeta grabados en alto relieve en el plástico debe coincidir con el número de tarjeta impreso en el recibo de venta, con el número que muestra el terminal/POS y con el numero de tarjeta impreso en el papel de firma. El último grupo de dígitos grabados debe extenderse hasta el holograma.

Verifique el número de la tarjeta

Los caracteres y números grabados en alto relieve en el plastico deben distinguirse claramente y su tamaño, así como los espacios entre los caracteres, deben ser uniformes.

Revise el holograma

Las tarjetas poseen un holograma que parece tener tres dimensiones al rotar. La mayoría de las tarjetas falsificadas llevan una imagen unidimensional impresa en un papel metálico.

Compare el número impreso

El número de cuatro dígitos impreso en el plastico (encima o debajo del número de cuenta de la tarjeta grabado en alto relieve) debe coincidir con los cuatro primeros dígitos del número de de la tarjeta.

Revise el panel de Firma

El nombre de la tarjeta suele ir impreso en un ángulo de 45 grados el panel de firma a prueba de falsificación

Fechas de validez

La Fecha de Vencimiento ("Good Thru") indica hasta cuándo se puede usar la tarjeta. Algunas tarjetas tienen también una Fecha de Validez ("Valid From"), que indica cuándo se puede comenzar a usar la tarjeta.

Compare la firma

La firma que aparece al dorso de la tarjeta debe coincidir con la que aparece en el recibo de venta. Todas las tarjetas deben estar firmadas.

Revise el símbolo respectivo

Las tarjetas suelen traer un símbolo grabado en alto relieve en la misma línea en que aparecen las fechas de validez.

Si por cualquier motivo sospecha que la tarjeta no es legìtima, llame al Centro de Autorizaciones, solicite un "Código 10", o siga las instrucciones suministradas por su banco.

comercio de parte de las bandas clonadoras o eviten participar conscientemente en tales operaciones.

Otro elemento, de carácter sociocultural, se vincula a la poca cultura de prevención por parte de los usuarios. El uso de medios electrónicos y su creciente sofisticación exige un manejo inteligente y racional por parte de los usuarios de los mismos. El manejo descuidado de claves secretas de tarjetas de débito que quedan expuestas al público, o el manejo atolondrado de los propios medios electrónicos, pérdidas frecuentes, facilitan la tarea de los delincuentes informáticos porque ponen a disposición de éstos el insumo principal con que trabajan, que es la información personal o financiera del usuario.

Resulta prioritario entonces hacer un esfuerzo para crear una cultura en el público, una mayor conciencia en la administración de los medios de pago. Las empresas y el propio Estado pueden emprender campañas para elevar el nivel de conocimiento y valoración por parte de los ciudadanos de los medios electrónicos a fin de que éstos participen activamente en la prevención de tales delitos y no sean, como hoy, presa fácil de las redes delictivas ligadas a la informática.

IMPUNIDAD Y TRABAS LEGALES

La cultura de la impunidad que ha dominado la vida judicial en nuestro país opera aún con mayor fuerza cuando se trata de los delitos informáticos. Las policías se encuentran en un estado de rezago e indefensión ante el avance del delito electrónico, completamente desfasadas respecto a los recursos técnicos para su combate. El público ignora muchas veces los riesgos que corre. Los juzgados y fiscales carecen de capacitación y experiencia en la materia. No existe legislación ni penas que disuadan a los delincuentes, por el contario, el vacío legal crea un ambiente de libertinaje y anarquía en esta materia que favorece el auge delictivo.

Este vacío se expresa patéticamente en los informes de PTJ, por ejemplo, donde se sostiene que en las detenciones practicadas por

casos de delitos informáticos, los delincuentes puestos a la orden de la Fiscalía, aunque atrapados in fraganti en muchos casos, a las 48 horas son puestos en libertad, debido a los beneficios que brindan las leyes venezolanas. La imposibilidad de obtener pruebas, por desconocimiento o por complejidad de los medios utilizados, impide elaborar expedientes y abrir procesos concretos, lo cual favorece la reincidencia. Por lo demás, la ausencia de una base de datos o de un sistema de coordinación de información que vincule a los distintos organismos tampoco permite hacer seguimiento de este tipo de actividad delictiva.

Esta situación de debilidad institucional se manifiesta con claridad en el caso del polémico Código Orgánico Procesal Penal, el cual establece un término de tiempo de 8 horas una vez que se practica la detención, por ejemplo, de una persona con los equipos o las tarjetas clonadas. Sin embargo, esas ocho horas resultan en las condiciones actuales de los organismos policiales y judiciales un tiempo extremadamente corto para precisar con certeza el hecho delicitivo[7] . Este es uno de los puntos en lo que se basan precisamente los fiscales del Ministerio Público para de inmediato dar el beneficio que establece la ley a una persona que, a pesar de ser conseguida con los equipos y con las tarjetas, no se le puede probar el delito.

Por lo demás, aún en el caso de que el hecho pueda ser probado, se pasa a una etapa donde la Fiscalía, igualmente carente de recursos técnicos en la materia, se encuentra en minusvalía para llevar adelante la respectiva acusación, todo lo cual termina favoreciendo la ocurrencia y multiplicación de hechos delictivos debido a la clara percepción de que el Estado venezolano está absolutamente incapacitado para hacerle frente.

---

7 A este respecto, la PTJ se quejó ante la Comisión de que una dificultad adicional a la que se enfrenta es que cuando se lleva la pescadora ante los bancos, a título de colaboración, éstos no poseen los equipos necesarios para determinar qué información contiene la misma, la cual constituye prueba irrefutable del hecho delictivo.

EL TRABAJO DE LA ASAMBLEA NACIONAL

Debido a la importancia y la necesidad de crear una legislación sobre los delitos informáticos, la Asamblea Nacional de Venezuela creó el 21 de septiembre del año 2000, una Subcomisión Especial, dependiente de la Comisión de Finanzas, a la que le encargó la tarea de investigar los fraudes informáticos en el Sistema Financiero en nuestro país y proponer un proyecto ley que atienda esta problemática. Esta Subcomisión estuvo integrada por los Diputados Carlos Tablante Hidalgo, quien la presidió; Guillermo Palacios, Elías Matta, Héctor Vargas y Norberto Peña.

Desde su creación la Subcomisión ha llevado a cabo una rigurosa investigación manteniendo entrevistas y consultas con distintos organismos públicos y privados, expertos, investigadores y académicos, incluyendo instituciones financieras, empresas franquiciantes de tarjetas de crédito, organismos públicos de control financiero, policías, jueces y entes públicos de protección del consumidor, entre otros. Las consultas permitieron diagnosticar la realidad actual del problema en Venezuela, las medidas que tantos actores públicos como privados han venido adoptando, las respuestas dadas a los usuarios de los servicios financieros y víctimas en general de los delitos informáticos, así como constatar las debilidades, fallas y vacíos que presenta el Estado venezolano en la lucha contra estas nuevas modalidades delictivas.

El siguiente es un recuento sucinto de las principales entrevistas realizadas por la Subcomisión y de las ideas, criterios, análisis y recomendaciones más importantes aportadas por dignos actores:

Junta Directiva de la Asociación Bancaria de Venezuela. Dr. Juan Carlos Escotet, segundo vicepresidente y coordinador del Comité de Prevención para la Administración del Riesgo Electrónico. Expuso las distintas experiencias que han tenido en la investigación del fraude electrónico y el diseño de las acciones que han ejecutado, en la primera fase, para prevenir el fraude informático. Estas medidas se resumen en:

a.- Inversión de importantes sumas en el proceso de selección y

adiestramiento de personal para minimizar las posibles ocurrencias de infidelidades o negligencias. Todos los bancos lo realizan con presupuestos propios; ellos han venido invirtiendo fuertes cantidades, y a través de la Asociación Bancaria.

b.- Utilización de las instancias gremiales para profundizar en este tipo de programas, con el consecuente costo que es asumido por la totalidad de los actores.

c.- Revisión y actualización de normas y procedimientos operativos de control interno con mayor énfasis en los controles automatizados.

d.- Fortalecimiento tecnológico de las unidades destinadas a prevención y control de fraudes con tarjetas de créditos y débito.

El Dr. Escotet en su intervención sugirió la creación de programas de educación para comercios, destinados al conocimiento, por parte de los dueños y empleados, de las acciones que deben ejecutar cuando estén en presencia de lo que pudiera representar fraude.

Dentro de las sugerencias finales expuestas se encuentra también la importancia de promulgar una ley que sancione a los delincuentes del crimen organizado; donde se incluyan todos los actores que participan en este delito, penándolos según sus condiciones y responsabilidad y tipificando el delito de fraude electrónico con dispositivos de acceso.

De igual forma, la Asociación Bancaria propuso:

- Estructurar en la Superintendencia de Bancos una unidad de inteligencia financiera. A los comerciantes o industriales que se les dé el carácter de sujetos obligados y que se les impongan las normas para su protección con carácter de obligación legal.
- Resolver la ausencia de responsabilidad penal, y aumentar las penas de delito, aplicar la pena por confabulación, concertación o conspiración.
- Considerar la pena de decomiso y de destrucción de equipos destinados, pues si no se eliminan las herramientas serán

otros los actores, pero seguirán cometiéndose los delitos.

- Establecer controles en las aduanas para evitar el contrabando de dispositivos portátiles de lectura y de almacenamiento de datos contenidos en medios magnéticos o electrónicos—el caso especifico de las «pescadoras». Declarar ilegal su uso diferente para la cual fueron creadas.
- Reformar el COPP, en la dirección de los fiscales, en la investigación penal de policía, y en el rigor de los jueces para conceder la libertad provisional a este tipo de delincuente.

Asociación Bancaria de Venezuela. Dra. Beatriz Ditotto, coordinadora de un equipo multidisciplinario que investiga el fraude informático y jefe de la Cátedra de Derecho Penal Especial en la Universidad Católica Andrés Bello. Señaló que esta problemática, la cual se va masificando cada vez más, no es algo que concierne solamente al fraude informático, sino que va más allá de ello. La Dra. Ditotto hizo énfasis en la necesidad de crear un ordenamiento jurídico, pero que no esté limitado por lo que está siendo más evidente: el fraude informático; sino que se aborde como un problema mucho más general, como delitos informáticos. Citó algunos trabajos realizados por los distintos países en materia penal con relación a este tipo de delito. Manifestó que a pesar de que el delito informático puede realizarse por organizaciones, no es propiamente un delito que se circunscribe al crimen organizado, sino que es típico de individuos solitarios que pueden llegar a causar daños considerables.

Recomendó igualmente que se debe abordar la reforma integral del Código Penal, ya que los títulos del mismo se quedaron muy desfasados con relación al avance tecnológico del cual hace uso la delincuencia, por lo que se necesita elaborar, con un enfoque distinto, un proyecto de ley que esté acorde al momento, y prevea futuras conductas.

Area de Gerencia de Seguridad Bancaria. Milton Chávez, experto privado. Disertó profundamente acerca de la materia, sobre la definición

del delito informático, su evolución y las condiciones legales que existían en el ámbito internacional. Se proyectó a la Comisión un vídeo en el que se formula una serie de recomendaciones sobre el uso adecuado y preventivo de las tarjetas de crédito y débito

Area de Delitos Informáticos. Joselín Maica, experta. En un diálogo proactivo se pudo conocer las condiciones a las que se ha estado enfrentando nuestro país con relación al delito informático. Se informó detalladamente acerca de los medios utilizados por los delincuentes para clonar o copiar las tarjetas, y el modus operandi que usan tales sujetos.

Area de Delitos Informáticos. Tai-Ling Antonetti. En su participación se analizaron las medidas que se deben tomar con las tarjetas de crédito y débito; explicó algunos conceptos básicos del fraude informático, los detalles de las tarjetas para ser identificadas como auténticas; habló igualmente sobre la importancia de la tipificación de estos delitos, la labor que está haciendo la Asociación Bancaria en la preparación de los distintos comercios para enfrentar estas situaciones y sobre las medidas de educación al cliente en el uso de las tarjetas.

Instituto de Defensa y Educación del Consumidor (Indecu). Samuel Ruh, presidente del Indecu. Refirió las distintas reuniones que ha sostenido el Instituto con las entidades bancarias para analizar las posibles causas que han podido ocasionar las cuantiosas pérdidas que han afrontado tanto los usuarios como las propias entidades bancarias. El presidente del Indecu aportó datos estadísticos con relación a los fraudes y las estafas informáticas, dando a conocer los bancos que estaban siendo más afectados por los fraudes informáticos y las gestiones que habían llevado a cabo con la Policía Técnica Judicial.

Superintendencia General de Bancos y otras Instituciones Financieras. Dr. Alejandro Cáribas. Se enfatizó que el problema de la delincuencia

informática no era propio de una entidad, sino que constituía un problema social, ante el cual deben aunarse los esfuerzos de toda la nación. Expresó que la Superintendencia ha desarrollado diversas reuniones con la banca allí se acordó que la banca haría un esfuerzo económico importante para redimensionar la base tecnológica usada por ellos para incorporar un sistema de seguridad más efectivo y menos vulnerable que los utilizados hasta el momento. Informó que la banca contaba con suficientes recursos financieros para afrontar estos cambios tecnológicos, sin necesidad de que el Estado intervenga para ello.

También se enfatizó en el papel vigilante que deben tener no sólo las instituciones bancarias, sino también el propio usuario con relación al uso de las tarjetas, con el objetivo de minimizar los daños de los cuales son víctimas. Igualmente la Superintendencia sugirió a la banca ser más estricta en los mecanismos de selección de los empleados, ya que ellos son potenciales infractores.

Cuerpo Técnico de Policía Judicial. Comisario General Eliseo Guzmán; Comisario Israel Galindo, Jefe de la División General Contra Drogas, y el Comisario Luis Guanda Araujo, Jefe de la División Contra la Delincuencia Organizada. Una de las problemáticas planteadas por el Cuerpo Técnico de Policía Judicial fue la carencia efectiva de funcionarios dedicados exclusivamente a la investigación de este tipo de fraude. Manifestaron la inexistencia de una base legislativa sobre la cual enmarcar los delitos informáticos, lo que trae como consecuencia que en muchas ocasiones cuando logran aprehender a estos delincuentes, por no contar con un respaldo legal, dichos sujetos son puestos en libertad; incluso, muchos de ellos reinciden en el acto delictivo, debido a que conocen la falta de control que existe en nuestro país para registrar tales conductas.

Los representantes de la PTJ mostraron ante la Subcomisión los medios utilizados por los delincuentes para llevar a cabo sus fechorías. Consignaron un trabajo escrito donde exponían el diagnóstico, las modalidades de fraude con tarjeta, un esquema donde se representa por mes las modalidades de los delitos de fraudes y estafas con tarjetas de

crédito y débito, los equipos de clonación, ejemplos reales de tarjetas clonadas, las dificultades que entorpecen el curso de la investigación en este sentido, y las sugerencias realizadas por el CTPJ.

Master Card International, Inc. de Venezuela y Cámara Venezolana de Tarjetas de Crédito y afines. José Ramil. Expuso la problemática que afecta al sector prestatario de los servicios que realizan las tarjetas de crédito y débito. Igualmente señaló las modificaciones que en el futuro sufrirá este tipo de instrumento para minimizar el fraude electrónico, haciendo hincapié en la incorporación de un chip electrónico contentivo de la información requerida por los tarjetahabientes. Insisitió en que uno de los principales elementos sobre los cuales se debe trabajar es la creación de una conciencia por parte del tarjetahabiente con respecto a la seguridad de sus tarjetas.

Igualmente se entrevistaron con la Comisión los siguientes representantes de bancos e instituciones del gremio financiero.

- Laury M. de Cracco, representante de la Asociación Bancaria.
- Banco Provincial, gerente de seguridad José Rojas Díaz.
- Banco Mercantil, Douglas Issele.
- Banco Federal, Eliazar Liendo.
- Banco Unión, Ramón Rivero, Jesús Ascanio y Tai-Ling Antonetti.
- Banesco, Luis Mejías y Raquel Cabrera.

Además de estas consultas con representantes de organismos directamente involucrados en el problema, la Sub Comisión mantuvo reuniones y consultas permanentes con expertos y académicos del área que nutrieron profundamente la investigación y permitieron definir un panorama de las realidades y tendencias legales en esta materia, comprender la vinculación de los delitos informáticos a múltiples aspectos de la vida social y económica. Sus reflexiones aportaron valiosa información y constituyen base del análisis que condujo a la propuesta de este libro.

- Dr. Gregorio Quiñones. Abogado especializado en Derecho Penal, autor de *Cibernética Penal. El delito computarizado* (1989).
- Dr. Fernando Rodríguez. Abogado especializado en delitos financieros e informáticos.
- Dr. Jorge Luciani. Abogado. Especialista en Derecho Mercantil. Profesor del Postgrado de Derecho Mercantil de la Universidad Católica Andrés Bello.
- Dr. Bayardo Ramírez Monagas. Abogado, egresado de la UCV. Fue profesor de Derecho Procesal Penal. Ex presidente de la Conacuid. Corredactor de la Ley Contra las Drogas y de su reforma (1993).

Después del intercambio de informaciones con los especialistas e instituciones mencionadas, y las audiencias parlamentarias realizadas, la Subcomisión llega a las siguientes conclusiones y recomendaciones:

- Que la Comisión Permanente de Finanzas se dirija a la Superintendencia de Bancos para que conjuntamente con la Asociación Bancaria acuerden medidas de prevención para asegurar los bienes de los usuarios de las tarjetas de crédito y débito.
- Recomendar a la Comisión Legislativa que conjuntamente con el Tribunal Supremo de Justicia, impulse la actualización y aprobación del Código Penal en estudio con la finalidad de prever el contenido de las políticas de Estado frente a este tipo de delitos informáticos, electrónicos o telemáticos.
- Promover desde la Comisión Permanente de Finanzas, la discusión y aprobación, por parte de la Asamblea Nacional, de un proyecto de ley contra los delitos informáticos, proyecto en el cual la Subcomisión está trabajando conjuntamente con la Asociación Bancaria de Venezuela.
- Promover acciones de coordinación entre los gerentes de Seguridad Bancarios, la PTJ, el Ministerio Público y la Superintendencia de Bancos, con la finalidad de crear un sistema eficiente apoyado en la más moderna tecnología a

objeto de coordinar los análisis que permitan atender con políticas de Estado lo más variado de estos delitos.

- Exhortar al Ministerio del Interior y Justicia a objeto de que sea creada una división contra los delitos informáticos, adscrita al Cuerpo Técnico de Policía Judicial.

RONDA DE PRESENTACIÓN DEL PROYECTO DE LEY CONTRA DELITOS INFORMÁTICOS

La presentación del proyecto de la Ley Contra Delitos Informáticos ante distintos actores sociales, institucionales y privados tuvo el objetivo de persuadir y concientizar acerca de la necesidad de contar con un instrumento previsivo, fundamentado, completo, actual, adecuado a nuestra realidad y flexible, para garantizar una protección penal efectiva e integral. Al mismo tiempo se propuso vencer las limitaciones que, en el área informática, suelen caracterizar al sector jurídico en razón de la poca afinidad entre la formación tradicional de los abogados y el uso de las tecnologías de información.

1. Superintendencia de Bancos (reunión con el Dr. Alejandro Cáribas, presentación a la Consultoría Jurídica y posteriormente a todos los departamentos vinculados con el uso de tecnologías de información).
2. Cámara Venezolana de Empresas de Informática –Cavedatos– (presentación y entrega a la Junta Directiva y a su asesor, Dr. Fernando Fernández).
3. Venamcham (presentación y envío del proyecto a una representación de distintas empresas).
4. Escritorio Jurídico Torres, Plaz & Araujo, asesores del Ministerio de Ciencia y Tecnología (entrega del proyecto para observaciones, lo cual generó una invitación del Ministerio para presentar el proyecto en un futuro evento en el mes de junio).
5. Fiscalía General de la República (reunión con la directora general, presentación a una representación de la Gerencia de Infor-

mática y abogados especializados y entrega del proyecto para discusión).

6. Cuerpo Técnico de Policía Judicial (presentación al director general y jefes de divisiones y envío del proyecto para observaciones y discusión).
7. Alcaldía Metropolitana (presentación al secretario de Seguridad Ciudadana).
8. Tribunal Supremo de Justicia (reunión con magistrados de la Sala Penal para realizar la presentación y entrega del proyecto en la última semana de mayo).
9. Circuito Judicial Penal del Area Metropolitana de Caracas (entrega del proyecto para observaciones y discusión al presidente del Circuito).
10. Comité de Riesgo de la Asociación Bancaria (presentación y envío del proyecto).
11. CONATEL (envío del proyecto al director general).
12. Empresas de telecomunicaciones (Telcel). Envío del proyecto a miembros del departamento de seguridad.

SUBCOMISIÓN DE FRAUDES INFORMÁTICOS DE LA ASAMBLEA NACIONAL

Visión de sus integrantes

Diputado Norberto Peña. Uno de los grandes problemas que se presenta en el país frente a los delitos informáticos es que, al no estar tipificados, el delincuente actúa con mucha libertad, provocando que este fenómeno se convierta en un efecto multiplicador. La banca debe asumir una transformación, quizás hoy el costo del fraude todavía sigue siendo manejable; es pequeño con respecto al costo de inversión de la nueva tecnología. Por ello es importante crear algún tipo de incentivo fiscal para que la banca se comprometa a asumir ese costo de inversión tecnológica, y a la vez facilitarle cierto tipo de exención

fiscal en los próximos tres años como una manera de contribuir a bajar sus costos, a bajar las tasas de interés que tanto afectan a los venezolanos.

Diputado Guillermo Palcios. Es necesario buscar nuevos mecanismos legales para poder enfrentar la situación social que están creando los Delitos Informáticos. Del mismo modo para llevar a cabo una labor efectiva en este sentido resulta de trascendental importancia que los distintos organismos e instituciones (PTJ, Indecu, Superintendencia de Bancos, la Fiscalía, etc.) trabajen en total armonía, y estén intercambiando constantemente la información y los resultados de su empresa.

Diputado Héctor Vargas. Es necesario que se tomen las medidas pertinentes para orientar a los usuarios y comerciantes vinculados a las tarjetas de crédito y débito para que de esta forma se aminoren las posibilidades de la comisión de tales delitos. La Asamblea Nacional está en absoluta disposición para brindar todo el apoyo necesario en la lucha contra los delitos informáticos.

Diputado Elías Matta. En el mundo están siendo discutidas las nuevas tecnologías. La Banca debe entender que estamos en un proceso de cambio tecnológico muy violento y que las personas lo están asimilando rápidamente para avanzar y mejorar su calidad de vida. Por eso es fundamental legislar en materia de penalidad con relación al delito informático, y considerar que, definitivamente, la tecnología usada en el país es obsoleta; hay que ir en la búsqueda de tecnologías más modernas y actualizadas, que verdaderamente puedan ser menos fáciles de vulnerar.

PROPUESTA DE LA ASAMBLEA NACIONAL

Propuesta de la Asamblea Nacional (realizada a finales de pasado año 2000) para ser incluida en el articulado de la Ley Habilitante con relación a la reforma de la Ley de Bancos y otras instituciones financieras:

Es necesario un control estatal para lo que se ha convertido en un problema de carácter social para el usuario, e instrumentar por esta ley la Unidad Nacional de Inteligencia Financiera, que ya existe y opera en la Superintendencia de Bancos. De esta manera se le garantiza estabilidad y seguridad legal, siendo la Unidad Nacional de Inteligencia Financiera una dependencia que controle y fiscalice en los bancos, otras instituciones financieras y casas de cambio, las normas de protección y seguridad que por resolución imponga Sudeban para minimizar y administrar el riesgo de fraude con dispositivos de acceso, cheques u otros instrumentos bancarios, electrónicos e informáticos; facilitando la fiscalización de la prevención y control sobre estos instrumentos bancarios, que permitan garantizar al pueblo la confianza y credibilidad debidos en la utilización de tales dispositivos, ya que hasta ahora el Estado ha sido negligente en este aspecto.

Artículo sugerido:

El Ministerio de Finanzas contará con una Unidad Nacional de Inteligencia Financiera, UNIF, la cual estará adscrita a la Superintendencia de Bancos y otras instituciones financieras, y será el organismo central nacional encargado de solicitar, recibir, analizar, archivar, y tramitar ante las autoridades de investigación penal competente y a los fiscales del Ministerio Público, la información financiera que requieren para realizar sus investigaciones, así como los reportes de actividades sospechosas sobre legitimación de capitales que deben efectuar a estos organismos de investigación penal los sujetos obligados por ley sobre Sustancias Estupefacientes y Sicotrópicas y otras leyes.

En esta unidad se creará una dependencia dotada del personal e infraestructura técnico-organizativa idóneos para cumplir con las mismas funciones en materia de fraude electrónico, por dispositivos de acceso y otros instrumentos bancarios con tecnología electrónica, cibernética o de informática utilizada por el sistema bancario y financiero de acuerdo a las normas de cuidado, protección, defensa y seguridad que les impongan las leyes o las resoluciones de la Superintendencia de Bancos y otras instituciones financieras como ente regulador del Estado. Las funciones y atribuciones específicas serán dictadas por resolución de este ente regulador.

Debe crearse con rango legal la Unidad de Inteligencia Financiera adscrita al Ministerio de Finanzas de la República Bolivariana de Venezuela, y que esa unidad de Inteligencia Financiera pueda ser el inicio de una política de Estado frente a este tipo de delito, el lavado de dinero, la legitimación de dinero, relacionado con el tráfico de drogas pero también con la corrupción, con el tráfico de armas, con todos los delitos relacionados con el crimen organizado.

La criminalidad informática y la estafa a través de Internet

Jorge Luciani Gutiérrez[1]

«La criminalidad evoluciona y se transforma
en la misma medida que lo hace la sociedad»
Emil Durkheim

Es un hecho que la sociedad evoluciona y se transforma. Vivimos cambios importantes en nuestras costumbres y formas de vida, fundamentalmente determinados por el desarrollo de la tecnología informática. La informática ha penetrado todos los ámbitos del quehacer humano, hasta tal punto que nuestra sociedad se ha convertido en totalmente dependiente de los computadores (como los llamamos en Latinoamérica) u ordenadores (como prefieren llamarlos en España). Pero recientemente y ante el asombro del mundo entero, las transformaciones se tornaron aún más radicales con la aparición de una herramienta informática conocida como Internet, que combina «poder de información con poder de comunicación», imponiendo de esta forma una nueva realidad, signada por dos conceptos muy actuales: lo virtual y lo global.

En efecto, Internet ha determinado cambios en distintos ámbitos de la vida humana, son millones sus usuarios en todas partes del mundo, además advertimos, que existen infinidad de bienes y servicios que se ofrecen y pueden ser comprados a través de la «red», lo que la ha transformado, de eficiente medio de comunicación a mercado global altamente apetecido por todo comerciante e industrial moderno. Es por ello que hoy en día, es necesario conocer y manejar esa «super-autopista de información», estar conscientes del poder que otorga a quienes la saben utilizar, pero también es menester conocer de las inconsistencias que presenta y los riesgos que deben asumirse al momento de su utilización.

---

1 Abogado. Especialista en Derecho Mercantil. Profesor del Postgrado de Derecho Mercantil de la Universidad Católica Andrés Bello.

Con la presencia de Internet, y tratándose de una sociedad que valora altamente la información, han surgido dos categorías de individuos: unos, los que poseen información, y otros, los que necesitan de ella y están ávidos de obtenerla. Estos últimos pueden dividirse a su vez en dos tipos, aquellos que utilizarán únicamente medios lícitos para conseguirla y los que a diferencia de los primeros, utilizarán cualquier medio para hacerse de ella y lograr su fin. Y es precisamente a este segundo tipo de individuo que dedicaremos parte de este estudio, porque interesa aproximarnos a conocer sus motivaciones y las causas que determinan su proceder.

Era de esperarse que frente al uso normal y perfectamente lícito del espacio informático surgiera, inevitablemente, el fenómeno social de utilización indebida, fraudulenta o criminal. Así, hemos podido constatar diversas modalidades de ilícitos, y muy especialmente la ocurrencia de variadas técnicas de fraude y estafa a través de Internet. Individuos y corporaciones en distintas partes del mundo han sido víctimas de estos procedimientos, en gran medida porque Internet, como lo ha señalado el brillante intelectual Juan Luis Cebrián, no es otra cosa que «una poderosa autopista de información desprovista de señales de tránsito», de manera que son muchos los desafueros que cometen los usuarios o «cibernautas» en la «red», y no menos frecuentes, los abusos que consuman oferentes y demandantes de estos bienes y servicios.

Si a esto agregamos la vulnerabilidad intrínseca que han demostrado estos instrumentos, y la falta de una regulación de carácter supranacional que supla ese vacío o falta de normas, pues estamos ante un terreno abonado que favorece la comisión de muchas y muy variadas formas de fraudes y estafas a través de Internet. Nuevamente estamos ante retos concretos que se plantean al Derecho Penal de hoy. Esta situación alcanza una importancia sin precedentes, dependientes como son nuestras sociedades de los ordenadores y de los espacios informáticos. Razón tenía Durkheim al decir que la criminalidad evoluciona y se transforma en la misma medida en que lo hace la sociedad.

Es por ello que en el presente estudio queremos abordar conceptos básicos de Internet, haciendo énfasis en sus elementos y herramientas,

con el objeto de entender cabalmente su funcionamiento, pero también lo que implica su utilización indebida, criminal o delictiva. Luego vamos a comentar aspectos de interés relacionados con la criminalidad informática, algunas situaciones de fraudes, estafas y otras manifestaciones de criminalidad que se producen a través de Internet y sobre todo buscando aproximarnos al «delincuente informático», en su manifestación individual y de grupo. Luego, ofrecemos un recuento a manera de «vuelo de pájaro» de los conceptos básicos del delito de estafa a la luz del Código Penal venezolano y buscaremos subsumir los supuestos de hecho planteados en el artículo 464 del Código Penal venezolano. Finalmente evaluaremos la posibilidad y necesidad de diseñar leyes con la finalidad de regular el tránsito de información en Internet.

LA CRIMINALIDAD INFORMÁTICA Y LA CRIMINALIDAD POR INTERNET

Para algunos, «criminalidad informática» y «criminalidad por Internet» son dos denominaciones referidas al mismo fenómeno delictivo, para otros la criminalidad informática es el género y la criminalidad por Internet la especie. No vamos a distraer su atención en discusiones bizantinas, en todo caso, todos están de acuerdo en sostener que la principal y por tanto más importante manifestación criminal a través de la tecnología informática, es la criminalidad por Internet. Luego de esto, debemos entender cómo funciona Internet, cuáles son sus herramientas, sus fortalezas y debilidades. Sólo así, podemos pasar a examinar las formas o modalidades de utilización indebida, las cuales en algunas oportunidades, podemos catalogar de criminales o delictivas.

INTERNET, UN ESPACIO INFORMÁTICO ABIERTO.

1.- Definiciones Básicas.

La combinación de tecnologías de comunicación como la del teléfono y la televisión con las de la computación o informática, con todo su poder de almacenamiento y procesamiento de información, presagiaban el nacimiento de una era con reglas y códigos nunca antes conocidos, que entrelazan a nivel mundial a todos aquellos que tengan acceso a la «red».[2]

Si añadimos a esto que hoy en día son cada vez más comunes los hogares con un PC, resulta que ese computador personal (*Personal Computer* o simplemente PC) se constituye en la llave mágica para todo un sin fin de posibilidades. No sólo se trata de la posibilidad de almacenar (de forma ordenada u organizada un cúmulo infinito de datos) y de procesar esta información, sino además se trata de la posibilidad de interactuar en una red internacional de información, denominada WWW, (siglas del término *World Wide Web*) o *World Wide Net*, comúnmente conocida como Internet.

---

2 En Juan Luis Cebrián, *La Red* (Editorial Taurus, Madrid 1997) encontramos «Hace algunos años hemos visto cómo las máquinas de escribir han quedado sustituidas totalmente por los computadores. Estos últimos facilitaban el trabajo de una manera increíble, no solamente cumpliendo con las mismas funciones de forma más eficiente y con mayores facilidades para el usuario, sino además, en ellas se podía almacenar información. En un primer momento los costos impedían que los cambios fueran tan drásticos, pero al poco tiempo, cuando estos se ajustaron, fueron precisamente los menores costos de las computadoras los que junto con sus otras ventajas determinaron cambios importantes. Luego, recordamos que estas computadoras, que más apropiadamente deberíamos llamar «servidores» estaban conectadas por una red a un cerebro central, que condicionaba sus funciones, su capacidad de respuesta, velocidad y poder de almacenamiento de información entre otras cosas. Poco tiempo se necesitó para que entraran en los mercados, con una fuerza inusitada, los computadores personales o simplemente «pc», que no requerían estar conectados a una red, y que dependiendo de su configuración hacían gala de gran rapidez y de excelente capacidad de almacenamiento o «memoria». Aún menos tiempo transcurrió para que ese computador personal cediera a la tentación de convertirse en uno de los instrumentos básicos de la globalización.»

2.- *¿Qué es Internet?*

Internet comenzó a gestarse en 1960 como un proyecto del Departamento de Defensa de los Estados Unidos de América, cuyo objetivo consistía en unir sistemas de información independientes con lenguajes incompatibles, establecidos en distintos lugares, dentro y fuera de los Estados Unidos de América, por intermedio de un idioma electrónico común y así poder intercambiar información a escala mundial. Desde entonces a la presente fecha, el proyecto no sólo dejó de serlo para convertirse en una realidad sino que ha crecido exponencialmente convirtiéndose hoy en día en un sistema global de información que une millones de pequeños sistemas de información en todo el mundo.

Para acceder a Internet lo único que se necesita es una línea telefónica y un PC con un *software* instalado. Efectivamente, «luego de concebir el hipertexto o esa poderosa autopista de información hubo que diseñar el instrumento para poder viajar o navegar a través de ella, lo que se logró con estos productos de software que constan de un navegador capaz de interpretar el lenguaje de la red y de traducirlo de forma inteligible para el usuario».[3]

La «web», por su parte, es una porción de la información disponible a través de Internet. Algunos la conciben como una colección o grupo de documentos «electrónicos» archivados o acumulados en computadores a lo largo y ancho del mundo. «La *web*, como universalmente se le conoce, es algo hecho a base de un cierto voluntarismo de los usuarios, aunque naturalmente ha sido ocupada por las grandes multinacionales y por los dueños de los servidores, los ordenadores que operan como incipientes reguladores del tráfico».[4]

A través de la conexión, los documentos o información contenida en la *web* pueden ser enviadas a computadores en distintas partes del mundo, con una rapidez de segundos, y por el costo de una

---

3 *Ibídem*, pág. 49.
4 *Ibídem*.

llamada de teléfono local. Las hojas *web* constan de gráficos y demás señas y textos que identifican a su propietario, pero también pueden contar con *hyperlinks*, que no son otra cosa que espacios resaltados, (a través de gráficos de colores mas fuertes, entre otras formas) dentro de la propia hoja «*web*», pero que tienen la función de servir de ventana de entrada a información adicional o a otras páginas *web*.

Mención adicional merecen los *e-mail* (o correo electrónico), que constituyen la razón de ser de Internet, ya que consisten en un medio de envío y recepción de mensajes a través de los millones de usuarios de la red. Así, cada usuario tiene asignado una dirección de e-mail o de correo electrónico (que cada quien libremente puede asignarse), que le permite recibir y enviar mensajes desde y hacia todas partes del mundo.

Por estas y otras características, Internet, en un tiempo sorprendentemente rápido, ha invadido todos los campos del quehacer humano. Y no podía ser de otra manera, ya que pudo conjugar poder de información con poder de comunicación. Esto nos lleva al punto siguiente, que consiste en repasar o hacer un breve recuento de lo que estamos viviendo con esta revolución de la informática y de las telecomunicaciones.

DE CÓMO ESTA NUEVA TECNOLOGÍA HA INVADIDO DIVERSOS CAMPOS DE LA ACTIVIDAD HUMANA

Así como a través de la prensa, radio y televisión se ofrecen bienes de muy distinta naturaleza y además se promocionan servicios de diversa índole, tal y como sucede por citar algún ejemplo, con los bancos y sus servicios bancarios, cuando anuncian las ventajas de sus «cuentas corrientes con intereses sobre saldos diarios», u ofrecen «tasas de interés a los ahorristas cuyas cuentas superen ciertos montos en depósitos»; así mismo también cada vez más productos, bienes o servicios se están promocionando a través de Internet.

Específicamente por intermedio de la hoja *web* de cada empresa ofertante. En efecto, bienes y servicios se ofrecen y además se pueden

comprar a través de la red, lo que la ha convertido, ya no únicamente, en un eficiente medio de comunicación y de intercambio de información sino en un mercado global (y virtual) altamente apetecido por todo comerciante e industrial moderno.[5] Esto ha sido una verdadera revolución.

De manera que hoy día somos testigos de la publicidad y del comercio que se está desarrollando a través de Internet. Hemos visto el reciente nacimiento de *e-commerce*, o comercio internacional a través de Internet, utilizando herramientas similares a los *e-mail*, a través de cuyas direcciones las empresas (comercios o industrias) venden y facturan sus bienes y servicios. Asimismo los bancos ofrecen la posibilidad del *home-banking* para que los clientes desde su propia casa u oficina puedan realizar sus transacciones y disfrutar de los servicios financieros de la institución. En Europa y los Estados Unidos de América, muchas empresas de seguros venden y renuevan las pólizas de sus clientes a través de ese servicio. Lo mismo hacen las bolsas del mundo desarrollada y vemos que se realizan miles de operaciones diarias de compra y venta de bonos, acciones y títulos por Internet. Todas las empresas, no importa al negocio que se dediquen, desean tener presencia en Internet.[6]

---

5 Hemos sido testigos de los distintos usos que se está dando a Internet. Por ejemplo, muchas empresas, comercios o industrias, han descubierto en Internet un espacio informático a través del cual no sólo pueden acortar distancias con el consumidor, sino además tener acceso a miles de millones de nuevos consumidores. Tal es el caso de las marcas de productos alimenticios las cuales, como todo comercio o industria que se precie de serlo hoy en día, cuentan con su hoja web, con el ánimo no solamente de anunciarse sino además de informar las ventajas de sus productos, los estudios que reflejan las propiedades alimenticias de sus productos y por si fuera poca cosa, Internet da la posibilidad de que los clientes de tales empresas se comuniquen con ellas y manifiesten sus puntos de vista con relación a la calidad de sus productos, o formulen sugerencias, o manifiesten sus reclamos. En otras palabras, conscientes que Internet llega a todas partes, es un medio o herramienta informático que permite tener más presencia, mejorar la comunicación con el consumidor, e informar innovaciones o planes futuros.

6 Por ejemplo, la empresa de juguetes norteamericana «Toys'R'Us Inc. Espera que sea un juego para niños desplazar para fines de 1999 a E-Toys Inc. de su lugar como el principal detallista de juguetes en Internet...» Más adelante se dice: «Estamos en el ciberespacio y seremos líderes del mercado. Para el cuarto trimestre esperamos ser el vendedor N° 1 de juguetes en la Internet» Concluye la nota de prensa diciendo: «Toys'R'Us Inc entró al negocio en Internet en 1998 para incrementar las ventas, después que fue desplazado por Wal-Mart como primer detallista de juguetes en EEUU». (tomado de el diario *El Universal* del domingo 13-06-99, cuerpo 2, pág. 2-14.)

Pero debemos estar alerta, de los muchos abusos que cometen oferentes y demandantes de bienes y servicios en Internet, y a través por supuesto de *e-commerce*. Son diversas y muy variadas las técnicas de fraude e inclusive fraudes estafatorios a través de la red. Son muchos los consumidores, en distintas partes del mundo que han sido víctimas de tales procedimientos. Lamentablemente, es muy poco lo que han podido hacer, para exigir responsabilidades de aquellos que los han defraudado o estafado.

En efecto, «frente al uso normal y perfectamente lícito del espacio informático surge como en todo el otro fenómeno social de su utilización fraudulenta o criminal».[7] Esto es un poco más un poco menos lo que sostenía Durkheim cuando dijo: «La criminalidad evoluciona y se transforma en la misma medidaen la sociedad» Internet es un fenómeno cultural y tecnológico que ha crecido invadiendo distintos ámbitos del quehacer humano, pues la criminalidad también alcanza a Internet como lógica consecuencia de su importancia y gran aceptación social. Esto nos lleva al tema de la criminalidad informática, que analizaremos a continuación.

LA CRIMINALIDAD INFORMÁTICA

En algunas modalidades delictivas, verdaderamente antiguas, pero muy de moda o en boga durante esta época de fin del milenio, como son los delitos de lavado de dinero o legitimación de capitales (nomen juris utilizado en Venezuela para este delito), se estudia mucho los *modus operandi* o mecanismos más conocidos o comúnmente utilizados para dar apariencia de licitud, esconder, ocultar o disimular capitales o bienes de procedencia ilícita. Decimos en tales casos que la delincuencia nos lleva una delantera (dos o más años de ventaja) porque mientras estudiamos procedimientos conocidos por todos que son utilizados para

---

7 Martin, Daniel, «Criminalité Informatique. Cybercrime, sabotage, piratage, etc. Evolution et represion». Editorial PUF, Press Universitaires de France, pág x. París, 1997.

este fin (o mejor dicho que utilizaron o ya dejaron de utilizar, para lavar dinero) seguramente al momento del análisis o antes ya se valen de nuevas técnicas o estrategias, no conocidas para lograr el mismo fin.

Considero que algo similar a esto sucede con la criminalidad informática. En materia de fraudes o estafas por Internet, la delincuencia dedicada a esto, nos lleva la delantera. Se trata de una manifestación delictiva altamente sofisticada (por el conocimiento exigido de los procedimientos y los sistemas empleados). Asimismo se dice que se trata de delincuentes astuciosos, (en muchas oportunidades lo que se producen son fraudes y estafas por Internet).

Otra peculiaridad que hemos encontrado es que no siempre con la comisión del delito se busca un interés económico. Aunque a veces sí como es el caso de los ejemplos que hemos planteado, pero en otras lo que sucede es simplemente ánimo de escandalizar, de sabotear.[8] Por esto, con la identificación de algunas manifestaciones delictivas y modus operandi utilizados en tales procesos se puede tener una idea (por lo menos una idea) de cuál es la naturaleza de los personajes que los ejecutan. Así, se han identificado algunas formas de utilización indebida de Internet, que en algunas oportunidades se constituyen en verdaderas actividades ilícitas o criminales. Éstas – simplemente para hacer la referencia y sin ánimo de desviar el objeto del estudio– podemos dividirlas en: a) actividades que configuran delitos contra la propiedad, b) actividades que configuran delitos contra la moral y buenas costumbres, y c) actividades que configuran delitos contra la privacidad de las personas y sus comunicaciones.

En el primer rubro, de delitos contra la propiedad podemos identificar todos aquellos que menoscaban patrimonialmente a otra persona. Nos referimos por ejemplo, a los fraudes en general por Internet, especialmente a los fraudes estafatorios, la piratería y el sabotaje entre otros.[9]

---

8 Ambos aspectos o características no las conocemos o son el producto de algún estudio estadístico, sino una inferencia en virtud de la publicidad que han hecho las víctimas de estas manifestaciones delictivas por Internet (conocimiento referencial).

9 Hoy en día en páginas especializadas de nuestros diarios de circulación nacional encon-

En cuanto a los delitos en contra de la moral y las buenas costumbres encontramos a la pornografía en todas sus manifestaciones, por Internet. Y en lo que se refiere a delitos contra la privacidad de las personas, podemos referirnos a la violación de mensajes e información que se produce a través de la red.

Existen muchas técnicas de fraude desarrolladas a través de Internet, que evidentemente «entrañan una lesión patrimonial». En efecto, podemos decir que la utilización de Internet, para realizar pagos o enviar mensajes importantes implica a su vez un sensible aumento de los riesgos de ocurrencia de fraudes o estafas, precisamente por tratarse de una red abierta, a la que tienen acceso millones de personas en todo el mundo.

En la actualidad, gobiernos y empresas utilizan Internet con la finalidad de mejorar sus servicios y para lograr mercados, respectivamente, pero el precio que se paga es que la seguridad de la información que manejan y de las transacciones que realizan se pierde en alto grado, si no se toman medidas de seguridad. En efecto, si no se toman medidas, la seguridad disminuye, porque existe la posibilidad de que alguien ajeno a los usuarios que se están comunicando, intercepte información perteneciente a ellos y la utilice con fines ilícitos. Igualmente la posibilidad de ocurrencia de fraudes aumenta mucho más si se trata de una utilización masiva, a gran escala como la que estamos viviendo. ¿Por qué? Porque Internet es una red abierta.

Por más seguridad que se imponga en una red de este tipo, su característica principal es precisamente, que estamos ante una red abierta. Para muchos de los especialistas y defensores de Internet, si se cierra la red, deja de ser Internet, y si se la regula, también, porque pierde algo de su esencia, cual es su característica de red abierta

---

tramos información como la siguiente: «Alerta Viral. Grandes empresas como Boeing, Intel, Microsoft y General Electric han tenido que desconectar su sistema de correo electrónico por un nuevo virus que se infiltra en el ordenador y tiene la capacidad de borrar archivos.»El nuevo tipo de virus que recibió un nombre y ha sido estudiado por empresas de seguridad de computación, fue catalogado como de «alto riesgo» , por su capacidad de destruir información (Tomado del diario *El Universal*, 13-06-99, cuerpo 2, pág 2-14)

desprovista de regulación. Muchos conocedores opinan que existe una verdadera anarquía internacional, creada por y a través de Internet, y esto es precisamente lo que constituye a esta herramienta informática en un terreno fértil para el fraude, razón por la cual debe sembrarse de leyes o regulaciones inmediatamente.

Dicho esto, pasaremos a comentar algunos aspectos de la modalidad de delito contra la propiedad a través de Internet, nos referimos al fraude estafatorio en Internet. Vamos a mencionar dos ejemplos de fraudes informáticos que se producen con mucha frecuencia, conscientes de la imposibilidad de abarcar las infinitas posibilidades de fraudes o estafas que pueda concebir la mente del «delincuente informático astucioso», pero que pueden darnos un ejemplo de ante quien nos enfrentamos. Estos hechos o fraudes estafatorios se producen manipulando indebidamente los *e-mail messages and pay* (correos electrónicos para mensajes y pagos) y los *e-mail transfer fund* (correos electrónicos para transferencia de fondos). Pero primero expliquemos la verdadera utilidad de estos instrumentos. Los *e-mail messages and pay* son utilizados como instrumentos para ordenar bienes y servicios y gestionar el pago de los mismos en el comercio internacional, en tanto que los *e-mail transfer fund* se utilizan como medio a través del cual muchos bancos e instituciones financieras en el mundo transfieren fondos entre bancos e instituciones financieras dondequiera que se encuentren en el mundo.

Pues bien, resulta que estas modernas herramientas electrónicas también han sido utilizadas como medios para la comisión de fraudes en general. Siempre interceptando primero la información valiosa que a través de estos canales se genera, y luego, utilizando la misma con el ánimo de engañar o sorprender en la buena fe a otro, induciéndolo al error, en procura de un provecho injusto en detrimento de alguna persona natural o jurídica. En otras palabras, siempre el medio o canal a través de Internet, es un *e-mail* o correo electrónico, en el que usurpando identidad se utilizan ilícitamente datos tales como números de cuentas bancarias, claves secretas, números de tarjetas de crédito, con la finalidad de girar

instrucciones para enviar dinero al destino que desea el estafador. Veamos algunos ejemplos.

En el primer caso estamos ante una persona, que como muchos de nosotros en estos días, manejando su PC accedió (gracias al *e-mail* o correo electrónico suministrado por una de las tantas empresas especializadas, que en Internet funcionan como un centro de datos parecido a una gran guía telefónica) a la página «web» de una conocida y muy seria librería, con sede en la ciudad de Nueva York en los Estados Unidos de América. El objetivo que se buscaba era consultar un listado muy amplio de libros a la venta, y eventualmente comprar unos libros editados en aquel país y escritos en idioma inglés. Luego de conseguir los libros de su interés, realizó la compra suministrando por Internet (a través del *e-mail messages and pay*) el numero de su tarjeta de crédito y todos sus datos personales. A los pocos días los libros llegaron a su destinatario, domiciliado en Caracas, Venezuela, quien maravillado por pertenecer a la aldea global permanecía ansioso a la espera de realizar nuevas compras a través de la red. Sin embargo, al poco tiempo desapareció el entusiasmo, cuando perplejo, frente al estado de cuenta de su tarjeta de crédito pudo constatar infinidad de compras, obviamente realizadas sin su conocimiento ni consentimiento, pero con la información que él mismo voluntariamente había suministrado a una dirección específica en la red.

Por lo tanto, se trata de una modalidad que consiste en interceptar información delicada o sensible a través de la red y luego utilizarla de manera ilegal con el ánimo de procurarse un beneficio propio o ajeno pero en detrimento del patrimonio de otra persona, natural o jurídica. De esta forma, interceptando la información de los *e-mail messages and pay*, se cometen fraudes que reportan importantes ganancias ilícitas para quienes han desarrollado esta modalidad delictiva.

El segundo ejemplo de fraude informático se produce manipulando los *e-mail transfer fund*, ya que previamente se ha interceptado la información necesaria, y consiste en, utilizando

Internet, hacerse pasar por el propietario de una cuenta y ordenar al banco realizar transferencias o girar instrumentos de pago a las direcciones o nombres que sean del interés de la persona que comete el delito o sujeto activo del fraude o estafa.

Con respecto a estos casos son muchas las preguntas que se formulan, por ejemplo no se duda que algún experto en la materia pueda penetrar las comunicaciones de la red y acceder a información con miras a cometer un fraude o estafa. Pero también se ha considerado seriamente la posibilidad de que existan personas infieles en instituciones como bancos y otros comercios de distinta naturaleza quienes serían los encargados de suministrar la información necesaria a aquellos que manipulan la red con ánimo de cometer fraude.

Luego de estas breves consideraciones, otra pregunta que surge es con relación a las características de esta criminalidad: ¿Se trata de una persona o se trata de un grupo organizado? Según lo que hemos investigado pueden darse ambos casos. A continuación vamos a analizar ambos supuestos.

EL CASO DEL DELINCUENTE INFORMÁTICO

Decíamos que estamos ante una manifestación delictiva de factura sofisticada, y astuciosa, en la que el ánimo de lucro no es una constante, salvo en los casos de estafas y fraudes en general por Internet. En efecto, a veces sí se evidencia un proceder ilícito, delictivo, dirigido a la consecución de una ganancia indebida, como en los ejemplos que hemos planteado. En otras oportunidades, lo que se produce es simplemente un ánimo de escandalizar o de sabotear, pero igualmente a través de la comisión de un delito, y aunque no se busque, en algunos casos igualmente producen un perjuicio económico.[10]

---

10 Hackers o Wackers es el nombre que le han dado a los que hacen sabotaje por Internet. Son individuos que penetran páginas «web» de entes públicos y privados y las modifican, haciendo gala de esta forma de sus destrezas en el manejo de esta tecnología.

Podríamos estar ante una persona con un nivel educativo medio o superior al medio, o por lo menos altamente especializado en el manejo de sistemas de computación y manejo a través de la «red», y en todo caso con conocimiento del lenguaje de la red o destrezas suficientes para entender o descifrar información. Es decir, se trata de personas con cultura informática y especialmente de delincuente informático. El tema de la cultura informática es interesante, porque podemos percibir claramente una vocación de asociación importante entre sujetos dedicados a estas actividades de manera profesional y lícita, asimismo entre aquellos que lo hacen por «hobbie» o distracción.

En relación con otra de sus características, su edad por ejemplo, no se ha podido determinar todavía cuál es el promedio de edad de estos delincuentes informáticos, pero en algunas oportunidades se ha podido establecer que se trata de menores de edad[11] muy diestros en manejo de computadores, introvertidos, solitarios que por distintos medios han logrado confeccionar o reunir equipos altamente sofisticados. El reto para estos jóvenes pareciera ser desafiar a los mayores, demostrarles que no existe un lugar de la «red» donde no puedan llegar. Este dato no es decisivo porque por otra parte, se han conseguido detrás de fraudes estafatorios o acciones de sabotaje de un «hacker», a una persona jubilada o retirada cuyas edades oscilan entre los 58 y 65 años de edad, cuyo *hobbie* es la computación y especialmente, navegar todo el día a través de la red.

En la mayoría de los casos estas personas permanecen anónimos o se protegen en el anonimato, porque utilizan un ordenador que no le pertenece o porque hacen ver que el autor de los delitos es otra persona. Esta habilidad para permanecer anónimos o para evitar que

---

En algunas oportunidades, el ánimo es simplemente sabotear, pero adicionalmente pueden causar daño patrimonial, ya que a veces dañan o estropean el computador receptor de su mensaje, o cuando menos se tiene que invertir nuevamente tiempo para solventar las consecuencias de su acción.

11 Nos referimos a menores de edad cuyas edades oscilan entre los 12 a 16 años de edad. Estas situaciones requerirían estudios mas profundos para determinar si se trata de travesuras que se pueden corregir y canalizar a tiempo o existe un problema de desajuste social, caso en el cual también debería tratarse.

a través de un seguimiento por la red puedan dar con ellos, revela además que estamos ante individuos que meditan previamente las consecuencias de su actividad criminal y evitan ser descubiertos. Para terminar también es importante acotar que en algunos casos de menores, y por situaciones como sabotaje o intercepción o sustracción de información a través de la red, se ha detectado afán protagónico o de fama por parte de ellos. No los mueve el «afán de lucro» pero sí los motiva altamente el «afán de notoriedad» o la fama.

CRIMEN ORGANIZADO Y CRIMEN INFORMÁTICO

Asimismo, y considerando que no se trata de tesis o posibilidades exclusivas y excluyentes, así como tenemos el delincuente informático como una persona que se vale de la tecnología informática, fundamentalmente de Internet para cometer diversas modalidades de delito, también podemos pensar que detrás de los fraudes y estafas por Internet está más de una persona que actúan como grupos de delincuencia organizada. En todo caso es una posibilidad cierta tomando en cuenta la importante cantidad de dinero que se consigue con esta modalidad criminal. En la organización criminal o delictiva cada quien ostenta su rol, las partes aportan su contribución en aras de conseguir el objetivo ilícito, existe el de adentro[12] y el de afuera, y

12 Nos referimos al *insider*, aquel individuo que trabaja dentro de una organización o empresa con el ánimo de conseguir información que luego será utilizada en una actividad criminal. Las empresas más buscadas por estos individuos son los bancos y otras instituciones financieras. Vale la pena destacar que las pólizas de seguro bancario, en todas partes del mundo, prevé estos riesgos y denomina esta actividad con el nombre de «infidelidad» y el que la realiza es identificado como el «infiel». Se ha podido comprobar por intermedio de infinidad de fraudes y estafas descubiertas, por este y otros medios, que se iban a perpetrar contra bancos, empresas de seguros, empresas bursátiles, casas de cambio, entre otros, que siempre existe un cómplice o alguien cooperando desde adentro, un «infiel». Hoy en día, los expertos en seguridad de las empresas se preguntan ¿Puede el «monitoreo» (*screening*) del empleado ayudar a anticipar el fraude? Los bancos conscientes del sacrificio en materia de seguridad habían consentido utilizar Internet como un medio más para mejorar sus servicios y acercarse al cliente, esto abrió la posibilidad de los fraudes y estafas bancarios a través de Internet.

además encontramos una jerarquía con distribución de funciones. Además de esto, otra característica es la permanencia, y por último el profesionalismo. Estos últimos elementos son muy importantes. Por ejemplo si se trata de una organización dedicada al contrabando, pues realizan la actividad ilegal con vocación de permanencia y con un conocimiento profundo del negocio, debe existir una organización jerárquica, cada quien cumpliendo su parte de la actividad de manera eficiente y altamente especializada. En esta materia de delitos informáticos, especialmente como los casos que sirvieron de ejemplos, bien podríamos encontrarnos a una organización dedicada a esto, es decir, en primer lugar unos a conseguir información tal como números de cuentas de banco, y otros se encargarían de realizar las operaciones por Internet, haciéndose pasar por los titulares de las tarjetas de crédito o de las cuentas bancarias. Pero todavía son muchas las preguntas que quedan por formular y sólo el tiempo permitirá responder: ¿Será posible entrar en la mente del delincuente, potencial estafador con la finalidad de entender mejor sus motivaciones y objetivos, y de esta forma diseñar mejores defensas contra su actividad?

Una vez que hemos revisado qué es Internet, su importancia y trascendencia como medio de comunicación masivo y a la vez como mercado global, las manifestaciones delictivas a través de la «red» y el delincuente informático; vamos de seguidas a pasar a la segunda parte del presente estudio que consiste en un breve recuento acerca del delito de estafa a la luz del Código Penal venezolano y luego buscaremos subsumir los supuestos de hecho planteados en el artículo 464 del Código Penal Venezolano a la luz de los delitos informáticos planteados. Finalmente evaluaremos la posibilidad y necesidad de diseñar leyes con la finalidad de regular el tránsito de información en Internet.

Son tantas las formas de fraudes y estafas en este campo como posible es imaginar por la mente humana un modus operandi o estrategia dirigida a un lucro indebido importante, y estos van desde la extorsión a través de la venta de información confidencial hasta fórmulas dirigidas a conseguir dinero por intermedio de la manipulación astuciosa de servicios de transferencias de fondos o pagos de tarjetas de crédito, penetrando la seguridad o defensas de Internet en estas materias.

EL DELITO DE ESTAFA A LA LUZ DEL CÓDIGO PENAL VENEZOLANO

El delito de la estafa según el artículo 464 del Código Penal de Venezuela

El artículo 464 del Código Penal de Venezuela establece que:

"El que con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole al error, procure para sí o para otro un provecho injusto con perjuicio ajeno, será penado con prisión de uno a cinco años. [13]

De la redacción del artículo 464 del Código Penal Venezolano podemos encontrar que son elementos constitutivos del tipo o requisitos fundamentales de la estafa:

a) Que el sujeto activo (estafador) utilice artificios u otros medios capaces de engañar o sorprender la buena fe de otro.
b) Que los artificios o medios capaces de engañar o sorprender la buena fe de otro, induzcan al error a otra persona.
c) Que los medios o artificios utilizados, para engañar o sorprender en la buena fe a otra persona, induciéndole al error, se conjuguen en procura de o para lograr la obtención de.
d) El provecho injusto con perjuicio ajeno».

Es importante hacer algunas aclaratorias. En primer lugar destacar que, «artificios o medios» pueden ser dos vocablos o términos lingüísticamente diferentes, pero jurídicamente indistintos, sobre todo tomando en cuenta la redacción del artículo 464 en comento. En este punto seguimos al Dr. Arteaga Sánchez, inclinándonos «por una visión amplia y de conjunto» porque tal

---

13 Compartimos con el Dr. Grisanti Aveledo, Hernando, que la redacción del artículo 464 es nefasta por decir lo menos, ya que la repetición de la palabra «otro» tan cercanas en el texto, y sobre todo cuando «ese otro es otro otro». Ver Grisanti Aveledo, Hernando, Ob. Cit. Pag. 300.

parece que insistir en las diferencias gramaticales contribuye más a la confusión que a aclarar la verdadera intención del legislador.[14] Asimismo la doctrina patria y extranjera además de la jurisprudencia venezolana han establecido diferencias entre las expresiones «capaces de engañar» por una parte y por la otra «o de sorprender la buena fe de otro», de manera que son dos supuestos distintos y por lo tanto considero importante insistir en la distinción. Es ésta la razón por la cual sostuvimos supra que la redacción del artículo 464 del Código Penal venezolano encierra en realidad tres (03) supuestos de hecho distintos. De la misma forma estamos ante un delito doloso en ambos sentidos, tal y como lo expresa el Dr. Grisanti Aveledo, porque dolo implica la intención de cometer el delito y porque al mismo tiempo dolo es además fraude o engaño.

Por lo que respecta al sujeto pasivo en el delito de estafa según el Código Penal Venezolano compartimos el punto de vista del Dr. Hernando Grisanti Aveledo cuando expresa: « La víctima del engaño es la persona que sufre el error...»[15] y nos permitimos complementar, «causado indistintamente por los artificios o medios utilizados por el sujeto activo o estafador». Más adelante continúa diciendo el Dr. Grisanti Aveledo: «El sujeto pasivo de la estafa es la persona perjudicada en su propiedad.»... El engañado y el sujeto pasivo de la estafa son cualidades que pueden recaer sobre una misma persona.[16]

En relación con el error, Grisanti Aveledo apunta refiriéndose al carácter doloso de la estafa, algo que nos permite recalcar la importancia del error cuando afirma: «el agente ha de obrar con la voluntad consciente (intención) de inducir a alguno al error...».[17] Por su parte, Arteaga Sánchez citando al tratadista argentino Ricardo C. Núñez recuerda que el error puede versar sobre «naturaleza, condiciones, causas o motivos de un determinado acto, sobre

---

14 Arteaga Sanchez, Alberto. En «La Estafa y Otros Fraudes en la Legislación Penal Venezolana» Editorial Jurídica Alva, S.R.L. 1981. Pags. 56 y57.
15 Grisanti Aveledo, *Ibídem*, Pág. 306.
16 Cfr.Grisanti Aveledo,*Ibídem*.
17 Grisanti Aveledo, Hernando, *Ibídem*.

las condiciones o cualidades de una determinada persona o sobre la naturaleza o cualidades de una determinada cosa»[18].

En todo caso el error debe producirse como consecuencia de la acción del estafador y debe fungir como causa de la prestación patrimonial de la víctima que además es la medida del perjuicio económico también característica de este tipo penal. «Si la prestación no se determina por el error que padece la víctima, no hay estafa»[19].

En cuanto «al provecho injusto y el daño ajeno» son elementos constitutivos del tipo penal de la estafa, o «requisitos fundamentales del delito de estafa» (Arteaga Sánchez). Esto quiere decir que si no se produce un «provecho injusto» no estamos ante una estafa. De la misma forma, si no produce un daño ajeno o perjuicio patrimonial a otra persona natural o jurídica no estamos ante una estafa. Este aspecto es de tal importancia, que inclusive se dice que «la estafa se consuma cuando el agente obtiene el provecho injusto con perjuicio ajeno (Grisanti Aveledo).

Posibilidad de subsumir los supuestos de hecho planteados en el artículo 464 del Código Penal venezolano

En los ejemplos comentados, tanto en el caso de la sustracción de información por Internet (a través del *e-messages and pay*) con motivo de la compra de los libros, como en el caso de las órdenes de transferencias de fondos y de giro de órdenes de pago producidas por la misma vía, (a través del *e-mail transfer fund*) el estafador ha utilizado, siempre Internet, manipulando «artificios o medios capaces» para producir un engaño o sorprender la buena fe de alguien, ya sea en el banco o en algún comercio, induciéndoles al error (el cual consiste en hacer creer al banco o comercio que se trata de la persona del cliente, que también se produce un provecho injusto con

18 Ibídem, Ob Cit. Pag. 72.
19 Ibídem, Alberto, Ob Cit. Pag. 73.

perjuicio o daño patrimonial ajeno, en la persona del titular de la tarjeta de crédito o de la cuenta bancaria según sea el caso. No obstante también debemos aclarar que, en ambos supuestos debemos distinguir dos momentos, el momento de la sustracción de información privilegiada y la posterior utilización indebida de la misma, inclusive usurpando identidades, porque los estafadores se hacen pasar por los titulares de la cuenta tarjeta de crédito o de la cuenta bancaria según el caso.

El problema se torna complejo cuando en ambos casos se busca determinar quién es el autor de los fraudes. Para identificar quiénes son los responsables, se requiere desplegar una actividad que resulta compleja y costosa, ya que el seguimiento a través de la «red» es difícil y altamente tecnificado, y luego al final del proceso, podemos encontrarnos con sorpresas como, por ejemplo, que en los dos fraudes intervino un ordenador adquirido de segunda mano y ubicado en una oficina desierta en Hong Kong arrendada a una empresa *off-shore* domiciliada en alguna isla del Océano Pacífico.

Ambos ejemplos vienen al caso porque permiten desarrollar nuestras interrogantes, las cuales son: ¿Cómo determinar cuál es el derecho aplicable? ¿Cómo sancionar a aquellos que han hecho uso indebido de una información, con ánimo de defraudar, y así cometer un delito?

Por supuesto también traemos a colación el tema de la necesidad de regular, de diseñar y desarrollar normas «globales» que permitan establecer reglas de comportamiento, formas de actuar, procedimientos obligatorios y uniformes para la utilización de Internet, así como también las sanciones previstas para aquellos que las violen.

Así las cosas, no quiero abordar el siguiente punto sin hacer una breve mención de la llamada *mise en scéne* o montaje de una escena o creación de un aparato escénico. En efecto, cuando la doctrina explica la graduación de los artificios, éstos van de los más elaborados (mise en scéne) hasta los menos, como el silencio por ejemplo, pasando por mentiras, medias verdades, entre otras.

Carrara citado por Arteaga Sánchez, está de acuerdo con la doctrina francesa según la cual «no basta para constituir el fraude o engaño de la estafa, la utilización de simples palabras mentirosas, sino que se requiere algo material, un aparato escénico, un *mise en scéne...*[20]. Es por ello que nos preguntamos: ¿Qué mejor escenario para la comisión de un fraude o estafa informático que Internet? ¿Es que acaso este aparataje informático no sirve de escenario facilitador del fraude o estafa?

Visto esto vamos a plantearnos distintas variantes o situaciones hipotéticas, dentro del ámbito de los ejemplos planteados, para luego adentrarnos en las posibles soluciones de acuerdo al ordenamiento jurídico penal venezolano.

Especial referencia a estafas cometidas en Venezuela

El primer caso que vamos a plantear se circunscribe al ámbito nacional: ¿Qué sucede si los casos planteados se producen íntegramente en Venezuela?

De antemano debemos recordar el texto del artículo 3° de nuestro Código Penal que establece: «Todo el que cometa un delito o una falta en el territorio de la República, será penado con arreglo a la Ley venezolana.»

Pues, se trata de un supuesto que no presenta problemas salvo aquellas cuestiones de índole práctico, como decíamos, cuales son las consistentes en ubicar a los responsables haciendo previamente un seguimiento a través de Internet. Porque, si se logra determinar que el fraude se produce en Venezuela por un venezolano o extranjero, pues se deberán aplicar las leyes penales venezolanas con arreglo al artículo 3° del Código Penal de Venezuela. Así las cosas procedamos a introducir las variantes, para luego aplicar las normas respectivas.

En lo que respecta al caso de la compra de los libros por

---

20 Arteaga Sanchez, Ob Cit. Pág. 59 y 60.

Internet, si la información se intercepta en Venezuela y se utiliza indebidamente en Venezuela con perjuicio de una persona natural o jurídica, pues habría que analizar el caso en concreto porque si estamos ante supuestos en los que se utiliza la información haciéndose pasar por una persona titular de la tarjeta de crédito, y a través de artificios o medios capaces de engañar o sorprender en la buena fe, por ejemplo del funcionario que autoriza las compras en el banco o comercio, induciéndole al error, con el ánimo de procurarse un lucro en detrimento de otra persona, en este caso el verdadero titular de la tarjeta de crédito, pues se cumplen los supuestos del 464 del Código Penal Venezolano. En el segundo ejemplo, se maneja información conseguida de manera fraudulenta, como en el primer caso, a través de Internet específicamente de los «e-mail fund transfer». Se utilizan artificios o medios capaces de engañar o sorprender la buena fe de un tercero, en este caso el funcionario bancario, induciéndole al error, porque el empleado considera que autoriza al verdadero titular, y además, toda esa actividad desplegada por el estafador se realiza en procura de un provecho injusto con perjuicio ajeno. Nuevamente estaríamos ante la figura del fraude estafatorio o estafa, tipificado en el artículo 464 del Código Penal Venezolano.

Estafas cometidas a venezolanos o extranjeros en Venezuela desde fuera de Venezuela

Pero traigamos a colación los ejemplos utilizados, y formulemos la siguiente interrogante: ¿Qué pasa si venezolanos desde Venezuela realizaron transacciones por Internet, lo que permitió que fuera sustraída información importante, tales como números de tarjetas de crédito, claves telefónicas, números de cuentas bancarias, entre otros datos, y posteriormente resultan víctimas de estafas producidas desde el exterior, desde cualquier parte del mundo?

De antemano también, parece que no existe una salida a través del artículo 3 y 4 del Código Penal Venezolano. Precisamente el artículo 3 establece el principio de la territorialidad y estamos

ante un caso producido desde fuera de Venezuela. Tampoco es aplicable el artículo 4, ya que los supuestos contemplados no pueden ser subsumidos por el supuesto de hecho planteado.

¿Qué hacer? Porque los dos supuestos planteados como ejemplos pueden ser subsumidos en el tipo penal previsto en el artículo 464 del Código Penal venezolano, siempre y cuando las estafas se produzcan desde algún lugar fuera de Venezuela. Además, no estamos ante un problema surgido de la aplicación simultánea de varios ordenamientos jurídicos, ya que en todo caso sería aplicable únicamente aquel ordenamiento jurídico-penal que corresponda al lugar donde se produjo el hecho.

Necesidad de diseñar leyes con la finalidad de regular el tránsito de información en Internet.

La imposibilidad de sancionar a aquella persona o personas que desde fuera de Venezuela cometan un fraude o estafa a través de Internet, dirigido a una persona en Venezuela es un supuesto cuya sanción dependerá exclusivamente de la aplicación de la ley penal del país desde donde se produjo el fraude o la estafa.

Es por ello que insistimos en la necesidad del diseño de un texto supranacional, producto del concierto de muchos Estados, tal y como se hizo bajo el auspicio de la Organización de las Naciones Unidas con la Convención contra el Tráfico Ilícito de Sustancias Estupefacientes y Psicotrópicas, mejor conocida como la Convención de Viena de 1988.

Gracias a este documento los Estados firmantes se obligaron a dictar leyes en sus respectivos países que abordaran el sensible tema del tráfico ilícito de drogas y del lavado de dinero proveniente de estas actividades, pero observando principios y reglas uniformes de tratamiento con respecto a ciertos aspectos y definiciones, y en especial sobre situaciones tales como diseño de tipos penales diversos, extradición, intercambio de información en el campo policial y cooperación y asistencia mutua a nivel judicial. Esto ha permitido crear un frente común, con leyes que responden a principios uniformes y que permitan atacar globalmente un problema delictivo por lo demás organizado y globalizado.

Algo que obedezca a estos principios debe proponerse y promoverse a nivel de una instancia como la Organización de las Naciones Unidas (repetimos, tal y como sucedió con la Convención de Viena de 1988 contra el tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas) con miras a lograr un texto que obligue a los países miembros signatarios de un hipotético acuerdo a establecer normas y principios básicos de funcionamiento de este espacio informático abierto conocido como Internet, dirigido además a regular la convivencia de todos aquellos que lo utilizan, que se constituya en marco de referencia obligatorio para la solución de conflictos y para el establecimiento de responsabilidades civiles o penales de los transgresores, sobre todo cuando se trata de ofertantes y demandantes de bienes y servicios. Consideramos que es el único medio para lograr una uniformidad legislativa tendiente a erradicar inconsistencias e incoherencias existentes entre distintos ordenamientos jurídicos nacionales y sus particulares formas de penalización.

Se necesita un instrumento de rango internacional que unifique criterios y fórmulas de prevención, control y represión de fraudes (como la piratería y el sabotaje informático) y de estafas a través de Internet en los ordenamientos jurídicos de los Estados firmantes, incentive la cooperación internacional para sancionar estos delitos, erradique legislaciones complacientes y por sobre todo facilite la identificación, persecución y sanción de aquellos que cometen fraudes y estafas a través de Internet, practican la piratería y promueven el sabotaje de los sistemas informáticos a través de la red.

Este documento debe marcar el inicio de un proceso de movilización internacional contra estos delitos. Obviamente con estas regulaciones Internet ya no será la misma red, pero el propósito es loable y lo que se busca es mayor seguridad jurídica. En alguna oportunidad durante una conferencia internacional sobre el tema tuve oportunidad de conocer a un experto norteamericano, se trataba de Alan Brill, de la conocida firma de seguridad Kroll, quien es de la opinión que detrás de estos delitos cibernéticos o informáticos existen organizaciones que buscan información para

venderla, por lo tanto se trata de una manifestación delictiva típica del crimen organizado, en este caso de carácter informático. Finalizó su conversación diciendo que al crimen organizado se lo combate con organización y más organización, y éste no parece ser el ejemplo que estamos dando con Internet, ausente de normas y regulaciones. En otras palabras la delincuencia está organizada y cada vez se sofistica más y la sociedad está carente de organización y defendiendo manifestaciones importantes e interesantes como Internet blandiendo únicamente la bandera de la libertad.

En resumen seríamos partidarios de proponer y promover un documento que regule los siguientes aspectos como mínimo:

a) Definir una serie de conductas que sean objeto de represión penal (exigiendo en lo posible que las conductas sean definidas de igual forma en cada país firmante del futuro acuerdo).
b) Establecer criterios muy claros de cooperación internacional, que obligue al intercambio y suministro de información, e inclusive asistencia mutua en instancias policiales y judiciales, a través de canales regulares.
c) Establecimiento de procedimientos expeditos de extradición.
d) En resumen lo que se persigue es lograr legislaciones internas en distintos países, pero que aborden el tema con criterio uniforme, sin contradicciones.

Hemos dicho que Internet conjuga poder de información con poder de comunicación, pero también hemos insistido en recalcar que existe una verdadera anarquía en este espacio informático que es aprovechada por quienes utilizan Internet en forma lícita e ilícita «La información constituye el eje central de una batalla por el conocimiento que se libra entre los que poseen información y quienes buscan apropiarse de ella»[21], de cualquier forma y utilizando

---

21 Cebrian, Juan Luis, Ob Cit. Pag .102

cualquier medio. Es decir, los que buscan apropiarse de la información a través de medios lícitos, así como aquellos que están dispuestos a la comisión de fraudes o estafas, con tal de hacerse de la información deseada.

«Si en el caos informal de las infocarreteras no se establecen códigos de circulación y autoridades que los hagan cumplir, la desorientación del usuario puede llegar al paroxismo. Pero si se procede de esta forma, muchos verán levantarse de nuevo el fantasma de la censura, y una abdicación en la defensa de la libertad absoluta de los cibernautas.»[22]

22 Cebrian, Juan Luis, «La Red». Editorial Taurus,Pag. 70.

Legitimación de capitales y tecnología: Cárteles invisibles y clientes sin rostro

En febrero del 2000, un periodista mexicano consultó al embajador de los Estados Unidos, Jeffrey Davidow, con respecto a lo que hacía el gobierno norteamericano, en su propio territorio contra el narcotráfico, «ya que sólo parece haber cárteles de otros países». El diplomático respondió que en su país hay casi un millón de personas encarceladas por crímenes relacionados con el tráfico de drogas, y agregó que «un gran número de los peces gordos norteamericanos ya son miembros de nuestra población encarcelada... Pero el hecho fundamental que hay que reconocer es que los dueños, los gerentes más importantes en el mundo del flujo del narcotráfico son mexicanos, colombianos, dominicanos y rusos». Acto seguido, Davidow agregaba: «Así como el cuartel general de la mafia estaba en Sicilia, ya el cuartel general de los narcotraficantes está en otros países y México es uno de ellos. Esa es la verdad...»

Al expresar de esa forma su convicción de que las sedes del narcotráfico están en América Latina, el diplomático estadounidense no respondía sin embargo la crucial pregunta de cómo es posible coordinar desde nuestros países operaciones de tan vasto alcance y complejidad. ¿Cómo hacen entonces estos cárteles para limpiar o legalizar los fondos ilícitos que obtienen y burlar los mecanismos legales internacionales y nacionales, precisamente cuando existe mucha mayor conciencia internacional acerca de la naturaleza de las operaciones delictivas del narcotráfico?

Es aquí precisamente donde las tecnologías de la información han venido a constituirse en una herramienta de primera mano para todo tipo de operaciones de legitimación y blanqueo de dinero

ilícito. Como ya hemos afirmado, las herramientas digitales y las redes de información brindan un conjunto de potenciales ventajas a los delincuentes, ofreciendo nuevos espacios y oportunidades, así como recursos más flexibles, veloces e intangibles para cometer delitos, potenciando así la capacidad de acción de las mafias de la droga.

Hoy en día, las propias autoridades norteamericanas reconocen que el lavado de dinero mediante mecanismos electrónicos o cibernéticos constituye la técnica más reciente para la práctica de la legitimación de capitales ilícitos. Querámoslo o no, los medios digitales forman parte ya del arsenal de armas y herramientas del narcotráfico. Instrumentos nuevos y poderosos que desafían los límites de la capacidad de respuesta de las autoridades.

La propia dinámica digital ha permitido acuñar un término que tiende a popularizarse. Se habla hoy en medios policiales internacionales de los «Carteles Financistas» o «Cárteles invisibles» para referirse a las sofisticadas estructuras delictivas que operan en los centros de consumo de droga, es decir, fundamentalmente en Estados Unidos y otros países desarrollados, desde donde financian y dirigen las operaciones financieras de sus negocios ilícitos.

Gracias a una compleja infraestructura delictiva y al uso de poderosas tecnologías teleinformáticas, los Cárteles Invisibles se mueven en las redes de negocios, en el mercado negro y en los medios legales como la misma naturalidad. Ya no emplean a sus secuaces para trasladar dólares a los países productores de drogas en sospechosos maletines, aunque no por eso han abandonado la práctica del uso de «correos» y «mulas» para otros tipos de operaciones. Estos nuevos y sofisticados «lavadores» usan giros y transferencias bancarias. Mueven las ganancias ilícitas mediante el uso de numerosas cuentas bancarias, sistemas financieros y herramientas tecnológicas, bajo la apariencia de ganancias comerciales legales.

La propia Organización de las Naciones Unidas (ONU) estima que la Industria Transnacional Ilícita de la Drogas (ITID) moviliza anualmente unos 500 mil millones de dólares, mientras el

Fondo Monetario Internacional (FMI), estima que el lavado de dinero negro equivale entre un 2% y un 5% del producto interno bruto mundial.

Estos impresionantes montos son productos de las acciones delictivas de diversas organizaciones criminales internacionales: terrorismo, contrabando, extorsión, evasiones fiscales, tráfico de armas, secuestro, trata de blancas, corrupción. Se trata pues de un fenómeno global, una industria poderosa y cuyas ramificaciones y alcance aumentan a medida que se refinan sus procedimientos debido al uso de los avances tecnológicos.

Aunque actúan fuera de los estereotipos de violencia y perversión de los carteles tradicionales, los nuevos lavadores invisibles constituyen un peligro mucho mayor porque operan desde dentro de los propios sistemas legales, manipulándolos, aprovechando los vacíos legales, la falta de información y el rezago tecnológico de los gobiernos. El espacio virtual constituye así un campo propicio para el refinamiento e incremento acelerado de sus actividades delictivas, fuera hoy de todo control por parte de las autoridades.

EL MERCADO NEGRO: LA ECONOMÍA SUBTERRÁNEA DE LA DROGA

Uno de los mecanismos que se ha visto favorecido con el desarrollo de las nuevas tecnologías ha sido el del mercado negro de divisas, un sistema monetario paralelo que permite a los cárteles legitimar fondos provenientes del tráfico ilegal de estupefacientes sin correr los riesgos tradicionales.

A este respecto, el 30 de Agosto del 2000, el gobierno de Estados Unidos entregó un informe sobre la cooperación entre Estados Unidos y Colombia en la lucha contra el lavado[1] y la

---

1 En la legislación venezolana este delito es denominado legitimación de capitales.

falsificación del dinero. El objetivo era bien preciso: contrarrestar el lavado de dinero a través del Mercado Negro de Cambio de Pesos (MNCP), considerado el más grande túnel para la legitimación de capitales.

El mercado negro del peso ha servido como canal fundamental de las operaciones financieras ilícitas realizadas por los cárteles de la droga. Se estima que de 3 mil a 6 mil millones de dólares se lavan anualmente utilizando el mercado negro, el cual consiste en la venta de dólares provenientes del narcotráfico, mediante los llamados «agentes de cambio del mercado negro» de Colombia, México, República Dominicana, Venezuela, Argentina, o en cualquier otro país latinoamericano.

El Mercado Negro de Cambio de Pesos opera no sólo en el tráfico de drogas, sino también en actividades de evasión de impuesto, contrabando, importaciones y exportaciones ficticias, lo que incide negativamente sobre el sistema financiero legal y el crecimiento económico de los países.

El sistema funciona más o menos de la siguiente manera:

La droga es vendida en los Estados Unidos o en cualquier otro país. Para pagarle a su proveedor en Colombia, sin ser descubierto por el sistema financiero legal, donde quedan registradas todas las operaciones, el vendedor en los EUA contrata a un broker (corredor de Bolsa), quien se encarga de que el producto o las ganancias de la venta de drogas lleguen a los jefes de los cárteles.

- Para lograr su cometido, el broker en EUA, que por supuesto, no puede mandar los dólares por el sistema financiero legal a los barones de la droga, contrata a su vez a un «colega» del país productor, quien busca importadores, ansiosos de comprar bienes en Estados Unidos con dólares baratos. Los importadores pagan con pesos en Colombia. Mientras, en Estados Unidos, los dólares obtenidos por la venta de drogas son utilizados para comprar los bienes que se exportarán a Colombia.
- El broker coloca los dólares en el sistema para pagarle a

los proveedores de los bienes en Estados Unidos. Pero lo hace utilizando varios bancos con depósitos menores a 10 mil dólares que es el límite. Después puede emitir cheques o transfiere los fondos al proveedor de los bienes. Esto está integrado de tal manera que ni los dólares llegan a salir de EUA ni tampoco entran a este país pesos colombianos. Las operaciones se coordinan como si fuese una operación financiera normal, y los fondos se mantienen, por cada una de las partes, en sus respectivos países.

- Al final del proceso, el narcotraficante obtiene sus ganancias en pesos y los importadores también logran su cometido de comprar bienes con dólares baratos, mientras los vendedores americanos han «exportado» ciertos bienes que sirven para legitimar la operación.
- Los agentes del Mercado Negro de Cambio de Pesos utilizan instrumentos monetarios, girados contra dichas cuentas, para pagar las mercaderías en nombre de los importadores colombianos del mercado negro. Para ocultar las compras ilícitas de mercaderías, esquivar el reglamento y los derechos arancelarios de importación de Colombia, estos importadores proceden luego a contrabandear las mercaderías y venderlas en el mercado negro.

¿Pueden hacerse todas estas elaboradas transacciones sin la existencia de organizaciones criminales dedicadas al lavado de dinero y sin aprovechar los eficientes medios tecnológicos actuales? Definitivamente, no. La coordinación de este tipo de operaciones exige no sólo un claro conocimiento de técnicas financieras sino también del manejo de herramientas de tecnología que facilitan, agilizan y dan apariencia legal a las operaciones. De esta forma, minimizando los riesgos, los Cárteles Invisibles logran lavar importantes sumas de capital de origen ilícito.

EL CASO BONY
EL MERCADO NEGRO DEL CIBERESPACIO

Lucy Edwards, vicepresidenta de la División de Europa del Este de Bank of New York (BONY), su marido Peter Berlin, comerciante nacido en Rusia, y Aleksey Volkov, presidente de Torfinex Corp., una firma no autorizada de transmisión de dinero, fueron acusados el año pasado de cometer nueve delitos previstos en las leyes de Estados Unidos, incluyendo conspiración y lavado de dinero.

La pareja y tres compañías bajo su control (Lowland , Benex International Co., Inc., y BECS International, LLC) admitieron su culpabilidad, demostrando de esta manera la vulnerabilidad de la poderosa institución financiera. Durante 42 meses, a partir de 1996 y hasta el 2000, en más de 160.000 transferencias movilizaron unos 7 mil millones de dólares, los cuales eran transferidos después a cuenta *off shore*[2] a solicitud de bancos rusos y otros clientes que evadían impuestos.

Las investigaciones determinaron que el software del Banco (BONY) tuvo un rol protagónico en las transferencias de las abultadísimas cantidades de dólares. Una vez instalado en las sedes de las tres empresas involucradas, con una computadora colocada en Moscú, comenzó el plan conspirativo. Los mafiosos rusos tuvieron acceso a la información de las cuentas, y desde sus propios equipos, realizaron todas las movilizaciones electrónicas. Al parecer, los recursos «lavados» provenían de préstamos del Fondo Monetario Internacional a Rusia, administrados por el Banco Central de ese país.

Aún se investiga si el banco sabía que las transacciones involucraban ingresos de actividades ilegales. Es lo que en el argot judicial se denomina «ceguera intencional», forma de «evitar deliberadamente el conocimiento de los hechos». Las cortes de Estados

---

2 Cuentas especiales aperturadas en ciertos bancos que operan en paraísos fiscales y financieros, bajo especiales condiciones de rentabilidad y confidencialidad.

Unidos usualmente contemplan igualdad entre la ceguera intencional y el conocimiento pleno sobre el origen ilegal de dineros o sobre el propósito y naturaleza de una transacción.

CLIENTES SIN ROSTRO

El caso BONY es un ejemplo de la manipulación de las nuevas tecnologías de la información con fines delictivos. Hoy en día, es un hecho reconocido que la teleinformación le lleva la delantera a la legislación, a las policías y a los jueces. Mientras las instituciones financieras se lanzan al campo de la cibernética y la automatización de sus procesos, bajo la presión de la competencia global, y los clientes empiezan a usar estos medios sin mayor conciencia de los riesgos y amenazas, aún no se encuentran las fórmulas contra la vulnerabilidad de las transferencias electrónicas, y otras operaciones que involucran en uso de sofisticadas herramientas telemáticas.

Los avances tecnológicos, el dinero electrónico, Internet, la ciberbanca, las tarjetas inteligentes, sin duda, constituyen medios e instrumentos de avance, de grandes utilidades y de aprovechamiento óptimo del tiempo, pero también de nuevas e interminables posibilidades para el crimen organizado.

La Ciberbanca y el dinero digital constituyen procesos a la vez sencillos y poderosos que favorecen el intercambio anónimo y extraterritorial. No hay barreras, no hay fronteras, pero crece la sociedad de la sospecha. Muchos son los bancos, en el ámbito internacional y nacional, que están ajustando su infraestructura de servicios para actuar en el campo de la teleinformación. Existe la llamada Banca Electrónica o Banca On Line, mediante la cual un cliente puede desarrollar transacciones bancarias, a través de Internet o usando medios y procesos electrónicos, sin necesitar de visitar agencias o sucursales bancarias.

Ha surgido así una nueva expresión, «clientes sin rostro», para definir a aquellos cuyas actividades, perfil social y laboral son

desconocidos por las instituciones financieras. Realizan sus actividades financieras y comerciales empleando medios electrónicos, a través de los cuales llevan a cabo transferencias nacionales e internacionales. Gracias a las tecnologías digitales, la vieja relación cara a cara entre el cliente y el gerente o funcionario bancario da paso a una relación anónima entre clientes desconocidos y sistemas informáticos donde la confiabilidad no se basa ya en la tradición de una relación, sino en claves y códigos de seguridad.

De hecho, hay bancos que no existen físicamente, sino exclusivamente a través de Internet, verdaderas entidades virtuales cuya existencia sólo se manifiesta a través de su personalidad electrónica en la web. Por su misma naturaleza son organizaciones polijurisdiccionales y sobre las cuales no existen aún convenios o normas internacionales aplicables. Operan en un mundo donde cada día se crece el acceso a los medios telemáticos sin mecanismos de adecuada supervisión por parte de las autoridades.

Internet, además, ha facilitado la aparición de los denominados «paraísos virtuales», sitios o páginas web que ofrecen identidades y ciudadanías falsas, a través de una jurisdicción inexistente. Asimismo, existen casinos y salas de juego virtuales. Todos estos medios constituyen pasto ideal para la comisión de delitos.

Otro de los desafíos consiste en el surgimiento del llamado «dinero electrónico», el cual puede ser intercambiado mediante el uso de tarjetas inteligentes, computadoras o Internet. Una variedad de sistemas electrónicos de pago ocupa la aldea global. Bancos y otras instituciones financieras han estado usando estos sistemas modernos, conectados a redes de computadoras fiables, rápidas con un costo bajo para las transacciones y una mejor atención a la clientela, a quienes se les ofrece la seguridad de no llevar dinero en el bolsillo. Por sus características de intangibilidad, instantaneidad y anonimato, el uso del dinero digital puede prestarse a la comisón de delitos como el del lavado de dinero ilícito.

El Departamento de Justicia de los Estados Unidos y la Oficina Federal de Investigaciones de los Estados Unidos, al anunciar, en

mayo del año pasado, la apertura del Centro de Denuncias de Fraudes en Internet, destacaban que «el lavado cibernético de dinero es la técnica más reciente de lavado de dinero... Cuando el mundo físico del lavado de dinero comenzó a erosionarse, la tendencia a utilizar transferencias electrónicas (transferencias por cable), para evitar la detección, consiguió leales seguidores...».

Según los investigadores norteamericanos, el sistema de transferencia por cable o medios telemáticos (vía redes digitales de información) permite a las organizaciones delictivas y a los negocios legítimos y clientes individuales de los bancos aprovechar un conducto rápido y casi sin riesgos para movilizar dinero entre países.

En el universo virtual del ciberespacio, la demanda por parte de los consumidores de transacciones eficientes ha llevado al establecimiento del dinero en efectivo electrónico. El E-efectivo o dinero digital es un sustituto electrónico del dinero en efectivo. Al usar el efectivo digital, los valores reales se transfieren por medio de comunicaciones digitales en forma de representación de billetes y monedas individualmente identificados similar a números de serie del dinero físico. Estas transferencias digitales son anónimas.

Aun cuando los bancos cibernéticos que aceptan E-efectivo anónimo están de alguna manera sometidos a las mismas leyes y regulaciones que las instituciones financieras en el mundo tangible, el que lava dinero debe ser primero aprehendido. Los informes son inútiles, porque los bancos no saben cuáles son los fondos del que lava dinero. Este hecho permite el lavado anónimo de dinero.

El uso criminal de los medios digitales abarca también el uso de tarjetas robadas; la fabricación y utilización de tarjetas bancarias falsas; el robo y reuso de datos y códigos; el acceso fraudulento a las páginas de comercio electrónico; la utilización de datos digitales transmitidos por un terminal de pago (lectores de tarjetas inteligentes); la extracción de datos de una red telefónica hasta la intervención de una red para simular una ciberbanca o un comercio electrónico.

La delincuencia organizada actúa a escala internacional, para

legitimar el dinero sucio. Acumula datos pirateados. Abre millares de cuentas bancarias pequeñas para luego enviarlas hacia paraísos fiscales, donde es imposible actuar, debido a la protección del secreto bancario.

El anonimato es el mayor enemigo en la lucha contra el lavado de dinero mediante medios digitales. El cliente sin rostro puede ser el mejor aliado del crimen organizado. Los nuevos productos y servicios de la banca representan, al mismo tiempo, nacientes retos, que sólo podrán vencerse por la vía de la cooperación y la integración internacional. Tarjetas inteligentes, tarjetas internacionales de débito, cheques digitales, comercio electrónico, son servicios y productos financieros modernos que son manipulados ya por los delincuentes.

Uno de estos mecanismos son las llamadas tarjetas inteligentes, un plástico del tamaño de una tarjeta de crédito, empleadas para realizar diversas transacciones o pagos en comercios tradicionales o electrónicos, transporte público, escuelas, universidades, teatros, cines, servicios médicos; control de accesos; identificación y peajes. Poseen uno o más chips semiconductores de silicio. El chip puede tener dos funciones: ser un poderoso microprocesador o actuar como un chip de memoria.

La característica fundamental de las tarjetas inteligentes es su capacidad de autogestión y la posibilidad de brindar múltiples servicios en un entorno altamente seguro, pero también anónimo. Por su capacidad para guardar valores en cantidades ilimitadas, por su extraterritorialidad, constituyen también una herramienta para la legitimación de capitales.

Los servicios de seguridad de los Estados Unidos y de otros países están haciendo esfuerzos para poner al descubierto el uso de tarjetas inteligentes por parte de cárteles de las drogas. Su manejo supone la desaparición del papel moneda, por lo menos el uso corriente de éste. Con ello, los delincuentes tapan evidencia, ya que venden sus nefastos productos y se les paga con estas tarjetas.

Por su parte, las tarjetas internacionales de débito, permiten

gastar grandes cantidades de dinero, sin ningún tipo de sospecha. Los cheques digitales operan como los cheques de papel, la diferencia radica en la firma que, no es manuscrita, sino digital (mediante un código de encriptado), para tramitarlos por Internet. El cliente, en este caso, posee una chequera electrónica –realmente una tarjeta parecida a la de crédito– que se introduce en un lector incorporado a la computadora.

Las tarjetas de crédito también pueden servir para la legitimación de capitales. Estas se utilizan mediante mecanismos de pagos anticipados o sobrepagos, con el objeto de crear saldos a favor del titular. Pasado cierto tiempo, se pide la cancelación de la tarjeta a fin de obtener la devolución del saldo. Así, el dinero proveniente de la comisión de un delito, queda lavado, blanqueado o legitimado.

Como se ve, los nuevos medios generan a su vez cambios en diversas áreas y su impacto es difícil de prever con la óptica tradicional. La economía digital está transformando la forma conocida de hacer negocios, abriendo nuevas ventanas de oportunidades y generando al mismo tiempo novedosos espacios para los delincuentes, mientras los Estados se mantengan a la zaga del proceso.

A medida que avanza la tecnología, la economía se transforma y el Estado trata de actualizarse, los jefes de los cárteles de la droga, de las mafias, de las tríadas van dejando atrás la magnificencia y los métodos agresivos para asumir un modo de vida «más discreto» o «más ejecutivo». Se esconden tras enormes oficinas equipadas al más alto nivel tecnológico. Cuentan con asesores financieros, legales y fuertes conexiones con la economía «real» que les permite simular la legalidad de sus operaciones. La necesidad de legitimar el producto de la comisión de delitos transnacionales, ha hecho del lavado de dinero un proceso «cuidadosamente tecnificado».

La velocidad a que se están produciendo estos nuevos fenómenos exige igualmente respuestas inmediatas, coherentes y eficaces. Como afirma Mario Baizan, no hay tiempo que perder. El gobierno de los Estados Unidos renueva su equipamiento cada 18 meses. El crimen organizado renueva su equipamiento informático y de

comunicaciones en un lapso promedio entre tres y seis meses «y muchas veces consigue que sus «hackers» desarrollen programas capaces de adelantarse, ganándoles la iniciativa a la fuerza de la ley»[3]. No hace falta ser un experto para entender el estado de indefensión en que nos encontramos en países menos avanzados tecnológicamente y donde el nuevo conocimiento y la tecnología es muchas veces copiada y absorbida en una forma pasiva.

EN BUSCA DE UNA ACCIÓN COMÚN: LA ESTRATEGIA ANTILAVADO DE ESTADOS UNIDOS

Bajo la premisa de que «mientras no podamos luchar contra el lavado de dinero en todas partes, no lograremos el éxito total en nuestros esfuerzos aquí en nuestro país...», en marzo del 2000 los Departamentos del Tesoro y de Justicia de los Estados Unidos anunciaron la Estrategia Nacional Antilavado 2000.

Este plan tiene entre sus objetivos trabajar en conjunto con otros países (miembros del llamado grupo de Acción Financiera - GAFI) con el fin de «identificar y avergonzar» a aquellas naciones o gobiernos que permiten que prospere la actividad del lavado de dinero. La misma idea ha sido llevada al seno del llamado Grupo de los 7 países más industrializados (G-7) y a las principales instituciones financieras internacionales como el Banco Mundial y Fondo Monetario Internacional, como afirmó el Secretario del Tesoro norteamericano, Lawrence Summers, el 26 de octubre de 2000, ante la Conferencia Nacional sobre Lavado de Dinero.

La Estrategia Antilavado ha sido definida como plan agresivo, cuya finalidad es extender las investigaciones sobre lavado de dinero mas allá de los bancos, es decir, incluir instituciones financieras y negocios no bancarios.

---

3 Baizan, Mario. *Democracia y Crimen Organizado*. Investigación publicada por la Revista Latinoamericana de Temas Internacionales. «Archivo del Presente». Diciembre de 1997.

Efectivamente, en el mes de junio, el GAFI calificó a quince países como «no cooperadores» en los esfuerzos mundiales antilavado. El único país latinoamericano incluido en esta lista fue Panamá. Un mes después, el gobierno de Estados Unidos emitió notificaciones a las instituciones financieras que operan en su territorio, advirtiéndoles sobre las «serias deficiencias» existentes en los países incluidos en el dictamen del GAFI. La falla se centra, según la notificación, en los sistemas de información de actividades sospechosas.

Se estima que para este año, el Departamento del Tesoro podría aplicar nuevas regulaciones, que incluyen reporte de actividades sospechosas a empresas de seguros, agencias de viajes, casas de empeño y otros «proveedores de servicios financieros».

Por otra parte, a nivel micro, la estrategia dirige la visión gubernamental hacia abogados, auditores, contadores, proveedores de servicios de ciberpago y un amplio rango de negocios y comercios electrónicos.

Dentro de los esfuerzos de la iniciativa estadounidense destacan:

- Regulaciones finales sobre reportes de actividades sospechosas para casinos y clubes de cartas.
- Regulaciones para la industria de valores.
- Incrementar los recursos para realizar inspecciones, bajo el Acta de Vigilancia Bancaria (BSA), sobre lavado de dinero a casinos y negocios de servicios monetarios.
- Un estudio del Tesoro sobre cómo pueden ayudar los contadores y auditores a detectar e impedir el lavado de dinero.
- Una revisión de las «responsabilidades profesionales» de abogados y contadores sobre control al lavado de dinero.
- Un constante monitoreo sobre las nuevas tecnologías «particularmente aquellas relacionadas a Internet y tarjetas inteligentes» con el fin de detectar vulnerabilidades al lavado de dinero.

El Plan además contempla medidas y objetivos tales como:

- Identificar métodos utilizados por los «lavadores» para insertar en el sistema financiero los fondos provenientes de los mercados negros de cambio. Además de incrementar la coordinación de esfuerzos en materia de investigación.
- Intensificar la evaluación de los paraísos fiscales.
- Evaluar los resultados de los controles antilavado de los servicios financieros ofrecidos a través de Internet.
- Discutir medidas estrictas de control antilavado en la ONU.

CONTROLAR LA CIBERBANCA

Con relación a la ciberbanca y el dinero electrónico, los esfuerzos internacionales se dirigen básicamente a:

- Mantener un marco de reglas globales, es decir, coincidencias de normas, para minimizar los riesgos de lavado de dinero y fraude por Internet.
- Aplicación de tecnología para el conocimiento del cliente. Asimismo, monitoreo permanente de las transacciones en línea.

Sobre este particular, el gobierno de Estados Unidos creó el Centro de Denuncia de Fraudes en Internet, el cual le permitirá a los consumidores establecer comunicación en línea con las autoridades gubernamentales, para que respondan sobre actividades sospechosas. A través de la dirección electrónica www.ifccfbi.gov, se puede llegar al centro, en el que participan agentes del FBI. El Centro ha sido creado para identificar, rastrear las nuevas tretas de los delincuentes, ya sea en el ámbito nacional e internacional.

El Centro de Denuncia de Fraudes en Internet, operativo desde mediados del 2000, se ha trazado objetivos precisos:

- Elaborar una estrategia nacional para hacer frente al fraude en Internet.
- Preparar casos penales de fraude en Internet y lograr juicios contra empresas o personas, responsables de fraude.
- Prevenir las pérdidas económicas debido al fraude en Internet en los Estados Unidos.
- Establecer un banco de denuncia de fraudes en Internet.
- Recibir, analizar y referir a las agencias de aplicación de las leyes, toda actividad fraudulenta en Internet.
- Identificar las tendencias actuales del crimen organizado en Internet y elaborar técnicas de investigación para abordar los problemas que identifiquen.
- Rastrear las operaciones de fraude en Internet.
- Elaborar módulos de capacitación para la investigación.

ACCION DESDE LOS BANCOS

Mientras los gobiernos diseñan y redefinen políticas, el sector financiero internacional ha comenzado también a instrumentar medidas y acciones para enfrentar los ciberdelitos bancarios y el uso de los medios digitales para la legitimación de capitales fraudulentos. En una reunión llevada a cabo en la ciudad suiza de Wolfsberg, algunas de las entidades financieras más importantes definieron un conjunto de principios de acción a fin de combatir el delito de lavado de dinero a través de las instituciones bancarias y financieras.

Algunos de los más importantes bancos privados del mundo tales como ABN AMRO Bank N.V., Barclays Bank, Banco Santander Central Hispano, S.A., Chase Manhattan Corporation, Citibank, N.A., Credit Suisse Group, Deutsche Bank AG, HSBC, J. .P. Morgan, Inc., el Société Générale y el UBS AG, participaron del acuerdo, adoptado como una importante guía global para una sana conducta de negocios en la banca privada internacional.

Los llamados Principios de Wolfsberg contienen lineamientos

para la conducta de los bancos en una amplia gama de áreas y procesos que incluye entre otros aspectos:

Aceptación de clientes: Wolfsberg establece que el banco deberá orientarse a prevenir el uso de sus operaciones internacionales para propósitos criminales. El banco deberá empeñarse en aceptar solamente aquellos clientes cuyas fuentes de riqueza y de fondos puedan ser determinadas razonablemente como legítimas. La responsabilidad primaria para ello se sitúa en el banquero privado que patrocina al cliente para que sea aceptado. El simple cumplimiento de los procedimientos internos de verificación no releva al banquero privado de su responsabilidad básica.

Identificación de clientes: El banco tomará medidas razonables para establecer la identidad de sus clientes y beneficiarios y únicamente aceptará a los clientes cuando haya sido ejecutado totalmente este proceso.

Beneficiario / usufructuario: El acuerdo de Wolfsberg establece que el derecho de beneficio / usufructo debe ser establecido para todas las cuentas. Debe realizarse un estudio técnico de todos los beneficiarios / usufructuarios principales de acuerdo con los siguientes principios:

- Personas físicas: Cuando la cuenta está a nombre de un individuo, el banquero privado debe establecer si el cliente está actuando por sí mismo. Ante cualquier duda, el banco deberá determinar la facultad por la cual actúa el titular de la cuenta y en representación de quién lo hace.
- Entidades: Cuando el cliente es una empresa, como ser una compañía privada de inversiones, el banquero privado deberá reconocer su estructura de manera tal que pueda determinar al proveedor de fondos, a el o los principales propietarios de las acciones y a aquellos que tienen el control de los fondos, por ejemplo: los directores y aquellos

que tienen poder para dar órdenes a los directores de la compañía. Este principio es aplicable sin importar si el capital accionario está representado en títulos nominativos o al portador.

- Fideicomisos: Cuando el cliente es un fideicomisario, el banquero privado deberá analizar la estructura del fideicomiso de manera tal que pueda determinar el proveedor de los fondos (por ejemplo el fideicomitente), aquellos que detentan el control sobre los fondos (por ejemplo los fideicomisarios) y toda otra persona o entidad que tenga facultades para remover a los fideicomisarios.

Cuentas abiertas a nombre de administradores monetarios e intermediarios similares: El banquero privado realizará estudios técnicos sobre el intermediario y deberá establecer, a satisfacción del banco, que el intermediario tiene procedimientos de evaluación técnica de sus clientes o una obligación normativa de ejecutar tales estudios técnicos.

Poderes / firmantes autorizados: Cuando un cliente designa un apoderado o un firmante autorizado, generalmente es suficiente con la realización del estudio técnico sobre el cliente.

Prácticas para clientes «de la calle» y relaciones originadas en banca electrónica: El banco determinará si los clientes «de la calle» o las relaciones iniciadas mediante canales electrónicos requieren un mayor grado de análisis técnico antes de la apertura de la cuenta.

Evaluación técnica: Es esencial obtener y registrar información que cubra categorías tales como propósito y razones de la apertura de la cuenta, actividad prevista para la cuenta, fuente de riqueza (descripción de la actividad económica que ha generado el patrimonio neto), patrimonio neto estimado, origen de los fondos (descripción del origen y de los medios de transferencia de las monedas que son

aceptadas para la apertura de la cuenta), referencias u otras fuentes que permitan corroborar la información sobre antecedentes, siempre que estén disponibles, y obligatoriedad (salvo en ciertos casos) de una entrevista personal con el cliente antes de la apertura de la cuenta.

Responsabilidad de supervisión: Deberá ser exigible que todos los nuevos clientes y las nuevas cuentas sean aprobados por al menos una persona distinta del banquero privado.

Aceptación de clientes: Situaciones que requieren informes o atención adicionales.

Cuentas numeradas o con nombres alternativos: Las cuentas numeradas o con nombres alternativos sólo serán aceptadas si el banco ha establecido la identidad del cliente y del beneficiario / usufructuario.

Países de alto riesgo: El banco aplicará procedimientos de verificación minuciosa a los clientes y beneficiarios / usufructuarios residentes en países identificados por fuentes confiables como poseedores de estándares inadecuados contra el lavado de dinero o que representan alto riesgo respecto del crimen y la corrupción. Los mismos procedimientos serán aplicados a los fondos procedentes de tales países.

Jurisdicciones extraterritoriales («off shore»): Los riesgos asociados a las entidades organizadas en jurisdicciones extraterritoriales («off shore») están alcanzados por los procedimientos de verificación técnica descriptos en estos lineamientos.

Actividades de alto riesgo: Los clientes y los beneficiarios / usufructuarios cuya fuente de riqueza provenga de actividades conocidas como susceptibles de maniobras de lavado de dinero deberán someterse a verificación minuciosa intensiva.
Funcionarios públicos: Las personas que tengan o hayan tenido cargos públicos tales como funcionarios de gobierno, directivos de

empresas gubernamentales, políticos, dirigentes de alto nivel de partidos políticos, etc., sus familias y sus asociados cercanos deben ser sometidos a verificación minuciosa intensiva.

Actualización de archivos de clientes: El banquero privado es responsable de la actualización del archivo del cliente. El supervisor del banquero privado o una persona con facultad de control independiente revisará regularmente cantidades relevantes de archivos de clientes para asegurar su consistencia e integridad. La frecuencia de las revisiones dependerá del tamaño, complejidad y riesgo involucrados en la relación.

PRACTICAS PARA IDENTIFICAR ACTIVIDADES INUSUALES O SOSPECHOSAS

Definición de actividades inusuales o sospechosas: El banco deberá contar con políticas escritas acerca de la identificación y el seguimiento de actividades inusuales o sospechosas. Tales políticas deberán incluir una definición de qué se considera sospechoso o inusual y presentarán ejemplos de ello.

Las actividades inusuales o sospechosas pueden incluir:

- Transacciones de la cuenta u otras actividades que no resultan consistentes con los datos recopilados en la evaluación técnica.
- Transacciones en efectivo por encima de cierta suma.
- Transacciones «de paso» que entran y salen.

Identificación de actividades inusuales o sospechosas: Las actividades inusuales o sospechosas pueden ser identificadas mediante:

- Monitoreo de las transacciones.
- Contactos con el cliente (reuniones, debates, visitas en su domicilio o empresa, etc.).

- Información de terceros (por ejemplo diarios, agencias de noticias, Internet).
- Conocimiento interno del banquero privado sobre el entorno del cliente (por ejemplo situación política en su país).

Seguimiento de actividades inusuales o sospechosas: El banquero privado realizará un análisis de los antecedentes de cualquier actividad inusual o sospechosa. Si no se llega a una explicación razonable deberá adoptarse una decisión que puede involucrar continuar la relación comercial con un monitoreo más intenso, cancelar la relación comercial, o informar de la relación comercial a las autoridades.

El informe a las autoridades debe ser elaborado por la función de control y deberá notificarse a la dirección superior (por ejemplo Director Honorario de Contratos y Acuerdos, Director General Ejecutivo, Auditor General, Asesor Legal). Si así lo requieren las leyes locales y normas, deberán bloquearse los activos y las transacciones deberán someterse a la aprobación de la función de control.

Monitoreo: Debe ejecutarse un adecuado programa de monitoreo. La responsabilidad primaria sobre el monitoreo de las actividades de las cuentas corresponde al banquero privado. Este deberá estar familiarizado con las transacciones relevantes y con el crecimiento de la actividad de la cuenta. Deberá estar especialmente alerta de las actividades inusuales o sospechosas.

Responsabilidades de control: Una política estricta de control deberá establecer procedimientos estándar de control que deberán ejecutar los distintos niveles de control (el banquero privado, la unidad independiente de operaciones, Departamento de Contratos y Acuerdos, Auditoría Interna). La política de control deberá considerar aspectos temporales, grado de control, áreas que deben ser controladas, responsabilidades y seguimiento, etc.

Informes: Deberá existir un régimen regular de informes gerenciales sobre temas relacionados con el lavado de dinero (por ejemplo

cantidad de informes cursados a las autoridades, herramientas de monitoreo, modificaciones en las leyes y normas aplicables, cantidad y alcance de las reuniones de capacitación brindadas a los empleados).

Educación, capacitación e información: El banco deberá establecer un programa de capacitación sobre la identificación y prevención del lavado de dinero, destinado a empleados que tienen contacto con los clientes. Una capacitación regular (por ejemplo anual) deberá incluir cómo identificar y seguir actividades inusuales o sospechosas. Además, deberá informarse a los empleados acerca de los cambios más significativos en las leyes y normas contra el lavado de dinero.

A todos los nuevos empleados deberá suministrárseles lineamientos sobre los procedimientos contra el lavado de dinero.

El banco establecerá requerimientos para la retención de los archivos para todos los documentos relacionados al lavado de dinero. Los documentos deben quedar con el documento por un mínimo de cinco años.

Requisitos para la retención bajo registro: El banco deberá establecer requisitos para la retención bajo registro de todos los documentos referidos a actividades contra el lavado de dinero. Los documentos deberán ser conservados por un mínimo de cinco años.

Organización contra el lavado de dinero: El banco establecerá un departamento independiente, categorizado de forma adecuada, que será responsable de la prevención del lavado de dinero (por ejemplo Departamento de Contratos y Acuerdos, unidad independiente de control legal).

INICIATIVAS MUNDIALES

Expertos jurídicos de la Organización de Naciones Unidas (ONU) han expuesto una serie de medidas para penalizar las acciones de la delincuencia organizada, incluyendo los actos de corrupción que comprenden el soborno o la oferta de soborno a funcionarios públicos para que actúen de una manera contraria a sus deberes oficiales. De igual forma, los funcionarios públicos que solicitaran o aceptaran sobornos se expondrían a enfrentar cargos de corrupción.

Los expertos jurídicos aún debaten las medidas más eficaces para frustrar el blanqueo de dinero, pero las más reiteradas han sido:

- Abolición del secreto bancario.
- Prohibir las cuentas bancarias anónimas o las cuentas a nombres falsos.
- Establecer dependencias de investigaciones financieras para reunir, analizar y difundir información sobre el posible blanqueo de dinero y otros delitos financieros.

Por su parte, la Comisión Interamericana para el Control del Abuso de Drogas (Cicad) de la Organización de Estados Americanos (OEA) recomienda: «Prestar atención a los riesgos emergentes de la aplicación de nuevas tecnologías para lavar activos, entre las cuales se destacan, sin que la lista sea taxativa, la realización de transacciones bancarias y el juego de azar a través de Internet, las 'tarjetas inteligentes' y el 'dinero digital', así como la utilización de otras tecnologías que pudieran favorecer el anonimato de quienes realizan transacciones y tomar medidas para prevenir su uso en lavado de activo».

La OEA recomienda además, la creación de unidades para la recopilación de análisis y el intercambio de información, que, de acuerdo a las circunstancias o características de cada Estado, pueden ser llamadas: Unidad de Inteligencia Financiera, Unidad de Investigación Financiera, Unidad de Información Financiera o Unidad de Análisis Financiera.

MIRAR HACIA AFUERA, MIRAR HACIA ADENTRO: EL RETO DE LA COOPERACIÓN

Las organizaciones criminales, y dentro de éstas, la Industria Trasnacional Ilícita de las Drogas (ITID), forman parte de los fenómenos globales contemporáneos, que por su complejidad organizativa y su capacidad para encubrirse en actividades de apariencia legal, son de difícil detección.

Una de las consecuencias negativas de la globalización es que la ausencia de acuerdos y de estrategias comunes de carácter multilateral propician la impunidad de las acciones delictivas multinacionales. Los avances de la teleinformática en manos del crimen organizado han creado también problemas de jurisdicción e integridad territorial, como también de violación de soberanías.

La dimensión global de la delincuencia y su repercusión política, social y económica, sólo ha generado respuestas de acciones puramente represivas sobre los llamados escenarios de conflicto, concretamente en los países latinoamericanos donde existen extensos sembradíos de marihuana, coca y amapola: de producción y tráfico de drogas. Se ha colocado el énfasis sobre lo militar, sin análisis sistemático o multidimensional, por encima de cualquier otra estrategia operativa.

A pesar de los fallidos intentos de establecer una alianza militar multinacional, aún Estados Unidos persiste en intervenir en una situación compleja, sesgando la atención integral que exige el problema mundial de las drogas. Un escenario de conflicto con Estados Unidos no es la salida idónea, por cuanto debemos verlo como un aliado necesario y estratégico, en la lucha contra el crimen organizado, y de éste la Industria Transnacional Ilícita de las Drogas. El objetivo es contar con el apoyo de la potencia del norte, a partir de la concertación, a fin de lograr con todas las naciones del mundo una efectiva cooperación internacional.

El Plan que necesitamos armonizar los países latinoamericanos con Estados Unidos no puede encubrir torpezas, como tampoco evadir las responsabilidades que las partes tienen en el problema.

Necesitamos de una Alianza que entienda la globalidad del problema de las drogas, pero que al mismo tiempo entienda las características diferenciales. Si nos ubicamos en el problema de la legitimación de capitales, la intervención militar carece de sentido práctico, pues hoy sabemos que las organizaciones criminales están usando con mayor frecuencia el espacio virtual y los medios telemáticos, un escenario que parece no contar con jurisdicción ni con reglas internacionales que apoyen una acción conjunta.

La expansión y consolidación de la Industria Transnacional Ilícita de las Drogas se produce por el aumento constante de la demanda para el consumo de sustancias estupefacientes y psicotrópicas. Dentro de los mercados ilícitos, el de EUA resulta muy atractivo para las organizaciones del tráfico de drogas. Este mercado motoriza la demanda y el dólar es la droga de los cárteles criminales.

Si en América Latina hay producción y tráfico, también existen las peores consecuencias sociales, políticas y económicas de la llamada guerra contra el tráfico de drogas, producto de la aplicación de severas sanciones, a través de la certificación o descertificación unilateral para aquellos países que están cumpliendo o no con sus acciones para prevenir la producción, el procesamiento y transporte de drogas hacia los Estados Unidos.

La descertificación ha condicionado el voto de los representantes estadounidenses ante el Banco Interamericano de Desarrollo (BID), ante el Banco Mundial y otros organismos económicos y de apoyo social. ¿Cómo recurrir a los cultivos alternos, si se coloca a países latinoamericanos entre la espada y la pared? ¿Cómo disminuir las condiciones de pobreza y marginalidad si se sitúa a las mayorías en condiciones de exclusión económica y social?.

Pero también hay que reconocer que América Latina, sus países en conjunto, necesitan una visión y una misión estratégica sobre el problema mundial de las drogas, como problema político, como factor de corrupción, de desestabilización económica, de desequilibrio institucional y democrático, de vulnerabilidad de la soberanía e integridad territorial y como amenaza a la autodeterminación de los Estados.

Frente a este problema necesitamos desarrollar una estrategia de integración, en función de intereses comunes y de conformación de una fuerza capaz de consolidarse efectivamente hacia una cooperación que exija concertación con los Estados Unidos y el resto de los países del mundo, en contra del crimen organizado.

La tecnología en manos del crimen organizado requiere una orientación política, social y económica, pero no a través de estrategias desiguales que simulan la figura del embudo, sino a través de una cooperación activa, franca y abierta que permita fortalecer la prevención y actualizar los mecanismos de acción administrativa, policial y penal de forma simultánea, al tiempo que se plantean acuerdos internacionales efectivos.

LOS RETOS DE VENEZUELA

En función de la necesaria cooperación en los escenarios: mundial, regional y subregional, destacamos como asunto de Estado, los principales retos de nuestro país.

Ley contra el Crimen Organizado y la Corrupción, para no seguir siendo un país débil en esta materia y con lo cual se solucionarían problemas bilaterales con EEUU y otros países europeos, ocasionados por la ausencia legal de procedimiento de técnica policial, como la «entrega controlada», y el «agente encubierto y provocador».

Es fundamental incluir en el sistema jurídico la responsabilidad penal de las personas jurídicas y la figura del Decomiso Civil.

Igualmente tipificar el delito grave de legitimación de capitales para todos los delitos de delincuencia organizada, que incluya entre ellos a la corrupción administrativa.

Los cuerpos policiales como la Policía Técnica Judicial y la Guardia Nacional deben contar con unidades especializadas en delincuencia organizada y legitimación de capitales. Además de una infraestructura informática idónea para llevar los casos de

investigación de crímenes financieros y delitos informáticos.

El Ministerio Público, que por el Código Orgánico Procesal Penal, de sistema acusatorio formal, es el Director de la investigación penal. Garante social de que la acción penal será ejercida, debe tener un criterio definido en materia de crimen organizado y delitos informáticos. Asimismo una infraestructura técnica-administrativa, dotada de especialistas en investigación financiera y en Delincuencia Organizada.

En materia de Legislación, la lucha contra la legitimación de capitales no puede concentrarse sólo en el problema mundial de las drogas, porque constituye apenas un sector de la actividad del crimen organizado. Hay que tomar en cuenta delitos como el contrabando de armas, el tráfico de órganos, el robo de vehículos, el comercio ilegal de joyas y piedras preciosas, el terrorismo,el secuestro, la corrupción política y administrativa, entre otros.

Por otra parte, los sistemas operativos de investigación, por su dispersión, no han sido aptos para la determinación y precisión de delitos relacionados con la legitimación de capitales. Hay fragilidad y debilidad en la aplicación de las leyes, por deficiencias en los sistemas judiciales.

En el marco de la cooperación internacional, consideramos fundamental:

Prevención, Control y Sanción de la Legitimación de Capitales, a través de la homologación de leyes y normas dirigidas a su represión. Para ello deben conformarse equipos internacionales lo suficientemente capacitados con la finalidad de poder detectar las sofisticadas operaciones de legitimación de capitales, las cuales hoy en día se realizan en el sistema financiero mundial, utilizando para ello toda la tecnología que la informática ofrece.

Extender la penalización de la legitimación de capitales a otros delitos graves, además del tráfico de drogas, incluir secuestros, tráfico de armas, entre otros. Para ello se hace necesario, discutir y aprobar legislaciones contra el Crimen Organizado.

Realización de programas de especialización para policías en el

área de investigación financiera, con el compromiso de los Estados de no desplazar a otras posiciones a los funcionarios que sean formados en este campo, por cuanto ello permite la adquisición de experiencias y la sistematización de las actividades que se emprendan.

Establecer un compromiso para que en las legislaciones sobre Banca y Otras Instituciones Financieras se establezcan medidas de provisión para que los organismos de investigación penal, fiscales y jueces puedan acceder a informaciones necesarias, cuando existan sospechas de la comisión del delito de legitimación de capitales.

Intensificar la cooperación y la colaboración en el intercambio de información oportuna, en casos de actuaciones de investigación policial que abarquen varios países, para lo cual, como condición obligatoria, debe respetarse la soberanía y la integración territorial de cada nación.

Garantizar que en la expansión internacional de empresas, bancos y otras instituciones financieras, se exija el aval del país de origen sobre la naturaleza del capital.

Proyecto de Ley contra delitos informáticos

Beatriz Di Totto[1]

INTRODUCCIÓN

Durante siglos, el grado de poderío político–económico y el bienestar de las sociedades provino del éxito en la explotación de la tierra. No fue, entonces, sino hasta bien entrado el siglo XVIII cuando la revolución industrial cambió ese patrón, e inventos como la máquina de vapor, la electricidad y el motor de combustión interna, pasaron a ser, junto con los desarrollos tecnológicos que de ellos derivaron y que sirvieron para incentivar el desarrollo industrial, los indicadores fundamentales de la fortaleza económica y política de las naciones.

A partir de entonces, han sido las sucesivas innovaciones tecnológicas las que han marcado la pauta del progreso experimentado por los países. Desde ese impulso monumental generado por la revolución industrial, el mundo no había experimentado un sacudón tan formidable como el que esa nueva y explosiva revolución, la única y verdadera revolución del siglo XX –la de los chips, los satélites, las redes informáticas, las computadoras y los cables de fibra óptica– ha propinado a las relaciones humanas.

Pero el asombroso potencial provocado por esa revolución de la informática representa, sin embargo, serios riesgos, especial-

---

1 Beatriz Di Totto es abogada, egresada de la UCAB con postgrados en Ciencias Penales y Criminológicas (UCAB) y "Planificación Estratégica" (Instituto de Altos Estudios de la Defensa Nacional). Actualmente Jefe de la Cátedra de Derecho Penal Especial en la UCAB, y miembro del Consejo Editorial del semanario Quinto Día. Realiza el ejercicio libre de su profesión en el escritorio económico-jurídico Petrosini-Di Totto y Asociados.

mente para ciertos países que, como el nuestro, lucen cada día más distantes de las sociedades avanzadas del planeta. El peligro mayor radica en la profundización de la llamada brecha digital, capaz de causar una ruptura aún más aguda entre el conocimiento y la ignorancia, entre ricos y pobres, entre personas conectadas y desconectadas, entre países con vocación y capacidad de incorporarse al primer mundo y países con profundas limitaciones que los mantienen anclados en el atraso y la miseria, sin posibilidad alguna de salir de ambos.

No cabe duda, entonces, de la incidencia que la incorporación de las tecnologías de información ha significado para muchos países en materia de atracción de recursos e inversiones, en elevación del nivel de educación y capacitación de su población y, desde luego, en el mejoramiento de la calidad de vida de sus ciudadanos. Por todo ello, constituye un objetivo de primordial importancia, casi podríamos decir que de supervivencia, la instrumentación de políticas públicas que incorporen a la sociedad venezolana al uso masivo de tecnologías que le permitan acceder a la única forma posible, hoy en día, de alcanzar un crecimiento económico sostenido y así contribuir a la erradicación de esa pobreza crítica que agobia a buena parte de nuestra población.

Alentadoramente, Venezuela está dando los primeros pasos en la dirección correcta. El Centro Nacional de Tecnologías de Información, adscrito al Ministerio de Ciencia y Tecnología, ya tiene elaborado un proyecto con las líneas maestras del Plan Nacional de Tecnologías de Información, en el cual se reconoce que «en la nueva era de la sociedad del conocimiento, la información y el conocimiento son factores claves en los procesos de producción y creación de riqueza». Asimismo, se afirma que «Venezuela enfrenta el desafío de diseñar e implementar políticas y estrategias que faciliten el despliegue de una Infraestructura Nacional de Tecnologías de Información (INTI) y democratice el acceso a la información y el conocimiento, vía Internet, con la finalidad de avanzar hacia una sociedad del conocimiento y de la información.»

Pero todo esfuerzo que se emprenda en este sentido hace indispensable, desde ahora, la promulgación de un conjunto de instrumentos legales que proporcionen el marco institucional adecuado al desarrollo armonioso del sector y a su democratización y que –precisamente para lograr estos objetivos–, promueva al mismo tiempo las condiciones de seguridad que inspiren suficiente confianza tanto a los administradores de las plataformas que brinden servicios tecnológicos como al usuario en general.

Una iniciativa fundamental al respecto fue la puesta en vigor, desde el 28 de febrero de este año, de la «Ley sobre Mensajes de Datos y Firmas Electrónicas», promovida por el Ministerio de Ciencia y Tecnología, con el apoyo de Venamcham y Cavecom, cuyo contenido constituye un soporte jurídico fundamental para dotar de certeza a las transacciones electrónicas, conferir valor probatorio al documento digitalizado y así contribuir al desarrollo del comercio electrónico en el país.

Por otra parte, el trabajo conjunto desarrollado por la Sub-Comisión Especial de Investigación de los fraudes informáticos en el sistema financiero adscrita a la Comisión de Finanzas de la Asamblea Nacional, que estuvo presidida por el diputado Carlos Tablante, por una parte, y la Asociación Bancaria de Venezuela, por la otra, tuvo la virtud de identificar oportunamente, en el curso del examen de los factores involucrados en el problema grave pero puntual que fue objeto de la investigación, la presencia de una serie de conductas adicionales, tanto o más dañosas que el mismo fraude informático, pero atentatorias de otros bienes jurídicos tan importantes como la propiedad, y que requieren, dentro de una estrategia múltiple de acción para combatirlas, ser reprimidas mediante una ley penal.

Esta importante iniciativa dio lugar a un estudio de derecho comparado que nos encomendó la Asociación Bancaria. Sus conclusiones, unidas a los resultados de la investigación desarrollada por la sub-comisión parlamentaria dirigida por el diputado Tablante, puso de manifiesto la carencia total y, por ende, la necesidad de un

ordenamiento jurídico penal más amplio que una simple Ley contra el fraude electrónico, de modo que su alcance permitiera proteger también, entre otros bienes jurídicos, los sistemas que usan tecnologías de información en el sector público, en especial en aquéllos que manejan informaciones sensibles como lo son las relacionadas con la defensa y seguridad del Estado o que preservan bases de datos con informaciones reservadas de instituciones o grupos de personas (identificación personal, antecedentes penales, por ejemplo); pero no tan sólo ello, sino que la amplitud de objetivos necesariamente supuso que esta ley se concibiese para perseguir y sancionar también las conductas que, sea como medio o como fin, utilizan las tecnologías de información para afectar la propiedad ajena, violar la privacidad de las personas y de las comunicaciones, promover la pornografía infantil, violar los derechos de los consumidores y, en fin, dañar los sistemas cuyo cabal funcionamiento es lo que garantiza la eficiencia y operatividad de las organizaciones públicas y privadas y el libre desenvolvimiento de las personas naturales; en pocas palabras, que favoreciera la seguridad de las actividades con la cuales se promueven la evolución y el desarrollo del país.

El proyecto de ley no sólo fue concebido para la protección de los usuarios en general sin distingo alguno, en lugar de limitarse –como podía presumirse– a la salvaguarda de los intereses de un sector en particular, sino que, gracias a la expresa disposición de las entidades involucradas –la sub-comisión parlamentaria presidida por Carlos Tablante y la Directiva de la Asociación Bancaria y, desde luego, quienes participamos en la elaboración del proyecto, labor en la cual me acompañó la Dra. Magaly Vásquez González– su contenido ha sido ampliamente divulgado y sometido a consulta con numerosas instituciones públicas y privadas, entre las cuales se cuentan la Fiscalía General de la República, el Tribunal Supremo de Justicia, el Circuito Judicial Penal de Caracas, el Cuerpo Técnico de Policía Judicial, la Superintendencia de Bancos, Venamcham, la Cámara Venezolana de Empresas de Informática (Cavedatos),

asesores del Ministerio de Ciencia y Tecnología, ingenieros de seguridad de sistemas de empresas de telecomunicaciones, en fin, sectores cuyas experiencias y aportes fueron atendidos y van a contribuir decisivamente a que el proyecto, concebido como una Ley Especial contra Delitos Informáticos sea una herramienta de verdadera utilidad práctica.

El complemento ideal de la ley penal la constituirá la promulgación de un ordenamiento de naturaleza administrativa, cuyas regulaciones permitan garantizar unos estándares mínimos en cuanto a la integridad, confiabilidad, disponibilidad y auditabilidad de los sistemas, así como la preservación de los rastros electrónicos por un período prudencial de tiempo con el objeto de facilitar la «investigación forense en computación». Estas disposiciones, cuya configuración en un instrumento legal concreto está en proceso de elaboración, unidas al resto del ordenamiento que hemos reseñado, colocará a Venezuela en una envidiable posición de vanguardia en el mundo en relación con el necesario equilibrio entre la incursión en las tecnologías de información y las mínimas seguridades para su uso, de manera que logremos vencer la resistencia del ciudadano común a incorporarse a los retos tecnológicos y así poder disfrutar de la verdadera democratización de las oportunidades que nos depara el futuro.

EXPOSICION DE MOTIVOS

Consideraciones generales

En efecto, el legislador al prever los comportamientos convencionales pretendió proteger, entre otros bienes jurídicos, la propiedad, la privacidad de las comunicaciones, la propiedad intelectual, la autenticidad de los documentos, etc.; no obstante, no consideró que tales hechos podrían ser perpetrados a través de

medios informáticos, electrónicos o telemáticos, de allí que, al margen de las tesis que, aplicando una interpretación progresiva de la ley penal, pudieren inclinarse por la inclusión de esas conductas dentro de tipos penales tradicionales, cada vez más se observa que, ante las limitaciones impuestas por el principio de legalidad penal que proscribe la analogía y la interpretación extensiva, actualmente los legisladores de los diferentes Estados introducen modificaciones en sus Códigos Penales o, por tratarse de una materia tan dinámica y en constante evolución, propician la creación de leyes especiales, sustancialmente de naturaleza penal.

Hoy puede advertirse al hacer un examen de derecho comparado, la tendencia a regular una amplia gama de conductas en las que los sistemas que utilizan tecnologías de información son objeto de la comisión de delitos o se utilizan como medio de comisión de delitos de diversa naturaleza: patrimoniales, atentatorios contra la intimidad de las personas, la autoría intelectual, la propiedad industrial o la información, entre otros bienes jurídicos o, inclusive, cuando a través del uso de esa tecnología, se afectan los propios sistemas a fin de causar daño a una persona o su propiedad, como es el caso de la transmisión de virus informáticos. Sin embargo, tales legislaciones tienen como denominador común el haber abordado el problema sólo desde la óptica del bien jurídico que en un momento determinado ha resultado mayormente vulnerado, de allí que no se aprecie una regulación sistemática que proponga soluciones o por lo menos controles globales al problema.

Algunos han sostenido que en tipos penales tradicionales contemplados en las actuales legislaciones podrían subsumirse algunos comportamientos perpetrados en perjuicio o a través del uso de medios informáticos; tal es el caso de los delitos de estafa, hurto y algunas modalidades atentatorias contra el derecho de autor. A ello se opone que en esos delitos el legislador ha dirigido su acción a tutelar el patrimonio económico, por tanto, el hecho de que la información almacenada en la memoria de un computador o, en general, incorporada a un sistema que utiliza tecnologías de información no

sea materialmente susceptible de apropiación, conlleva a la imposibilidad de aplicación de tales dispositivos legales. Ni siquiera mediante la interpretación progresiva de la ley podría lograrse este cometido pues se vería seriamente afectado el principio de la legalidad.

Es así, entonces, que la conducta desplegada a través del acceso a un sistema que utilice tecnologías de información no podría encuadrar en un tipo penal tradicional, como el hurto cuando, por ejemplo, un sujeto conoce u obtiene la contraseña para penetrar en el sistema con el fin de que se verifique la transferencia de una cuenta bancaria ajena a otra creada por él. Dicha conducta difícilmente podría encuadrar en el apoderamiento de que trata el Código Penal máxime si la acción recayó sobre la información, independientemente de que los efectos y los fines sean de carácter económico. De la misma manera, en el supuesto en el que se manipule un sistema que usé tecnologías de información con el objeto de que reconozca y acepte una instrucción falsa y de esta forma obtener un beneficio económico que produzca a otro un perjuicio patrimonial, tampoco se materializaría el delito de estafa, pues conforme a la descripción contemplada en el Código Penal venezolano es necesario que se induzca a "otro" en un error, por tanto el sujeto pasivo de tal delito debe ser una persona y no un computador o un sistema que utilice tecnologías de información.

La legislación venezolana sanciona (Ley sobre Protección a la Privacidad de las Comunicaciones) la afección a la privacidad de las comunicaciones, no obstante, la punibilidad de esos comportamientos está supeditada a que se trate de conversaciones telefónicas. Ello supone que sería impune por falta de tipicidad, por ejemplo, el acceso sin autorización a un servidor de correo electrónico, pues en este caso, aún cuando hay una clara intervención, podría considerarse que no es propiamente telefónica sino que tal concepto fue rebasado por la participación de otros componentes propios de las tecnologías de información que son adicionales e imprescindibles para que ese mensaje de datos objeto de intervención pueda ser transmitido y recibido.

Lo anterior lleva a concluir la necesidad de tipificar en nuestro derecho interno una serie de conductas que, realizadas con el auxilio de medios informáticos, electrónicos, telemáticos –o, para utilizar el vocablo más actual en la materia, medios que supongan el uso de tecnologías de información– puedan afectar, entre otros bienes jurídicos, la propiedad, el derecho a la información, a la inviolabilidad del secreto, a la intimidad, al honor, todo ello en consideración a que el bien protegido puede desaparecer o ser seriamente afectado sin que el sistema usado como medio de comisión, sufra menoscabo alguno.

La proposición de una ley especial descriptiva de delitos informáticos requiere asumir una postura en cuanto al alcance del término. Ello significa que, en razón del tecnicismo y la dinámica tan veloz de la materia, se considera fundamental adoptar la nomenclatura más actualizada para prevenir la inaplicabilidad inmediata por falta de tipicidad en algunos casos o la obsolescencia prematura del instrumento legal y, al mismo tiempo, definir con claridad y exactitud cada uno de los términos novedosos cuya incorporación es imprescindible para que la ley cumpla su cometido: tecnología de información, sistema, data, información, documento, computador, *hardware, firmware, software*, programa, procesamiento de data o de información, seguridad, virus, tarjeta inteligente, contraseña o *password* y mensaje de datos.

Regulación en el Derecho Comparado

Internacionalmente puede advertirse una tendencia, acentuada en los últimos años, a legislar sobre la materia.

En Europa se aprecia el caso de Alemania, donde comenzó a regir, a partir del 1° de agosto de 1986, la Segunda Ley contra la Criminalidad Económica, instrumento en el cual se sanciona, entre otros, el delito de estafa informática y la utilización abusiva de cheques o tarjetas de crédito. Al mismo tiempo se tipifica la comisión de delitos convencionales como la falsificación o defraudación a través de medios informáticos, se trata, simplemente, de un cambio en el medio de comisión del delito.

En Austria se reformó el Código Penal el 22 de diciembre de 1987. En este instrumento se contemplan dos modalidades de delitos informáticos: aquéllos en los que la acción del autor va dirigida a destruir datos personales o los propios programas (destrucción de datos), y cuando se influye en una operación automática con el fin de causar un perjuicio patrimonial (estafa informática).

En Portugal, la Ley de Protección de Datos Personales Informatizados (29-04-91) sanciona, entre otras conductas, la utilización ilegal de datos y el acceso no autorizado a las bases de datos.

Por su parte, en Gran Bretaña se sanciona con privación de la libertad o multa el intento de alterar datos informáticos, independientemente de que tal fin se alcance.

En Holanda, la Ley de Delitos Informáticos (1-3-93) sanciona la utilización se servicios de telecomunicaciones evadiendo el pago total o parcial de dicho servicio, la inducción en error a fin de que el afectado suministre información que no aportaría en condiciones normales y la distribución de virus. Con respecto a esta última modalidad delictiva se admiten tanto la forma dolosa como la culposa.

En España, el Código Penal reformado en 1995 contempla una serie de conductas íntimamente vinculadas con la materia informática, es el caso, por ejemplo, de las estafas electrónicas, los daños informáticos, la interceptación de correo electrónico, la publicidad engañosa, la pornografía infantil y la revelación de secretos. Además en la actualidad se ha propuesto un Anteproyecto de Ley de Comercio Electrónico en el que se plantean severas sanciones pecuniarias para quienes incurran, entre otras conductas, en afección a las comunicaciones comerciales por vía electrónica o se violente el contenido de un contrato celebrado por esa misma vía.

En Francia, a través de la Ley sobre el Fraude Informático se sanciona además de la destrucción dolosa de datos, el acceso fraudulento a un sistema de elaboración de datos, la falsificación o uso de documentos (falsos) informatizados y el sabotaje informático.

En Italia, la descripción y sanción de los delitos informáticos

se encuentra contemplada en el Código Penal, instrumento que prevé, entre otros comportamientos, la falsificación informática, el acceso abusivo, el fraude informático, la violación de la correspondencia electrónica y la introducción de virus informáticos.

En América, Estados Unidos se ha incorporado a esa tendencia regulatoria. Así se advierte de su adopción del Acta Federal de Abuso Computacional de 1994 mediante la cual se modificó el Acta de fraude y Abuso Computacional de 1986. En tal Acta se sanciona con pena privativa de libertad a quienes hayan causado daño con la transmisión dolosa o culposa de un virus. Al mismo tiempo, el Estado de California adoptó en 1992 la Ley de Privacidad en la que también se contemplan delitos informáticos. En el mismo sentido, la legislación del Estado de Florida.

En Latinoamérica el interés en legislar sobre la materia también se advierte de manera insistente. Chile fue el primer país latinoamericano en sancionar una ley contra delitos informáticos. Tal instrumento legal comenzó a regir el 7 de junio de 1993 y sanciona, entre otras conductas, la destrucción o inutilización de datos contenidos en una computadora y la revelación maliciosa de datos contenidos en un sistema de información.

En Argentina aún no existe una legislación especial que sancione los delitos informáticos, sin embargo, mediante el Decreto 165/94 del 8 de febrero de 1994 se agrega a la lista de comportamientos referidos a la propiedad intelectual la protección a las obras, bases de datos y software.

Por su parte Colombia sancionó el 18 de agosto de 1999 la Ley 527 en la que si bien no se contemplan disposiciones penales, se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

En Perú, la Ley N° 27309 del 15 de julio de 2000, incorporó los delitos informáticos al Código Penal, tipificando la utilización o ingreso indebido a una base de datos, sistema o red de computadoras o cualquier parte de la misma, la interferencia, interceptación, acceso o copia de información en tránsito o contenida en una base de

datos. De la misma manera se describió la utilización, ingreso o interferencia indebida de una base de datos, sistema, red o programas de computación con el fin de alterarlos, dañarlos o destruirlos.

En México, específicamente en el Estado de Sinaloa, también se ha regulado sobre los delitos informáticos. En esta legislación, dirigida básicamente a proteger el patrimonio, se sanciona el acceso a una base de datos con el fin de defraudar u obtener información y la interceptación o destrucción de datos. Otra regulación vinculada con la materia se encuentra en la Ley Federal de Derechos de Autor donde se protege, bajo la amenaza de sanción, los programas de computación, las bases de datos y los derechos autorales relacionados con ambos. De la misma manera, el Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, sanciona como un delito contra la propiedad intelectual el uso de programas de virus.

De la relación anterior se deduce claramente la necesidad de que Venezuela se incorpore a este movimiento regulador de conductas atentatorias contra diversos bienes jurídicos (propiedad, honor, fe pública, intimidad, etc.) perpetradas a través de sistemas que utilicen tecnologías de información.

Necesidad de una ley especial

Lo complejo que puede resultar una modificación parcial al Código Penal, sin correr el riesgo de desnaturalizar su estructura, recomienda la elaboración de un instrumento especial destinado a regular los delitos informáticos, ello además por ser este último un procedimiento más expedito. No obstante, debe proponerse una regulación tan completa y desarrollada recogiendo las más modernas variantes que podrían contemplarse como delictivas a fin de que el instrumento diseñado, de advertirse una tendencia codificadora en un futuro, pudiere pasar a conformar un título o capítulo del Código Penal.

A estos efectos, el Proyecto que se propone adopta una serie

de disposiciones generales aplicables sólo a esta materia dadas las particularidades del delincuente informático, pues en algunos casos puede tratarse de un delincuente solitario que puede actuar con dolo directo o eventual en la medida en que dirija su acción a la afección del bien que se tutela o que previsto el posible resultado lo acepte, pero en otros, y dada la multiplicidad de bienes jurídicos que con su actuar pueden vulnerarse, se trata de verdaderas organizaciones delictivas que emplean los sistemas que utilizan tecnologías de información como medio para facilitarse la comisión de ilícitos. La propuesta que se hace contempla, además, la inclusión de comportamientos culposos.

El Proyecto aprovechó la experiencia del derecho comparado vigente y en proceso y, fundamentalmente, las modalidades dadas a conocer por Naciones Unidas, a saber:

a) Los fraudes cometidos mediante manipulación de computadoras.
b) Las falsificaciones informáticas.
c) Los daños o modificaciones de programas de datos computarizados

Estructura del Proyecto

El Proyecto de Ley que se propone consta de cuatro Títulos estructurados de la siguiente manera:

Un primer Título contentivo de las disposiciones generales en el que se precisa el objeto de la ley, se contemplan algunas definiciones básicas dado el carácter técnico de la materia. En razón de la dimensión transnacional del problema pues se trata de hechos que pueden cometerse de un país a otro, se incorpora una previsión sobre extraterritorialidad de la ley penal que permita a la justicia venezolana conocer de tales hechos punibles y, por cuanto algunos de los hechos punibles previstos en el Proyecto pueden ser perpetrados por intermedio de una persona jurídica o con el fin de que ésta reciba sus efectos o beneficios, se establecen los supuestos

que harían procedente su responsabilidad, la cual, en todo caso, sólo podría ser de orden pecuniario.

En el Título II se describen los delitos informáticos. Para la sanción de las conductas allí descritas se adopta el sistema binario, esto es, pena privativa de libertad y pena pecuniaria. Con relación a esta última se fijan montos representativos calculados sobre la base de unidades tributarias por considerarse que la mayoría de estos delitos, no obstante la discriminación de bienes jurídicos que se hace en el Proyecto, afectan la viabilidad del sistema económico, el cual se sustenta, fundamentalmente, en la confiabilidad de las operaciones.

El Título III, contentivo de las disposiciones comunes, comprende las circunstancias agravantes de la responsabilidad penal por los delitos que se proponen y el régimen de imposición de las penas accesorias.

En el Título IV se contemplan las disposiciones finales referidas a la vigencia de la ley y la derogatoria de las normas contempladas en otros instrumentos legales que puedan colidir con ella.

Visto que la propuesta que se hace es de un instrumento estrictamente penal, resulta pertinente dedicar algunas líneas al análisis tanto de los tipos penales como del sistema de penas concebido:

Delitos informáticos

Actualmente no es posible contar con una definición de delitos informáticos, pues cada país de acuerdo a sus realidades ha formulado un concepto en el cual de ordinario se procura incluir nuevas modalidades delictivas o describir en términos más actuales comportamientos tradicionales que, en razón del medio de comisión empleado adquieren la condición de informáticos. Sin embargo, al describirse el objeto de la ley, en el artículo 1° se está formulando un concepto de delito informático en términos bastante actualizados, al indicar la descripción, en términos generales, de las conductas que se pretende prevenir y sancionar en la Ley y al remitir al vocablo

tecnologías de información el contenido global de la informática con todos sus componentes.

Partiendo de la consideración anterior, el Proyecto procura agrupar en seis Capítulos en el Título II, una amplia gama de comportamientos discriminados en función del bien jurídico que, a través del uso de medios que utilizan tecnologías de información, resulta vulnerado.

En efecto, en el Capítulo I se describen una serie de conductas que atentan contra los sistemas que utilizan tecnologías de información: en el artículo 6 se castiga el tipo doloso de acceso no autorizado a dichos sistemas. Si bien esta modalidad no produce un daño a los sistemas su acceso a través del uso ilegítimo de password compromete seriamente la seguridad que el propietario quiso resguardar mediante la contraseña, de allí que se justifique su represión penal.

En la descripción típica del sabotaje o daño a sistemas (artículo 7) encuadran los daños que puedan causarse a un sistema que utilice tecnologías de información, con el fin de obstaculizar su normal funcionamiento. La peligrosidad de este comportamiento radica, entre otras cosas, en el hecho de que en la mayoría de los casos los signos visibles sólo se advierten cuando el daño ya se ha materializado. Se prevé la agravación de la pena cuando el daño se produce con ocasión de la creación, introducción o transmisión de un virus o programa análogo.

Podría considerarse que los daños físicos causados a los sistemas encuadrarían dentro del tipo penal de daño, mientras que tal postura es discutible con relación a los daños lógicos; no obs-tante, dado que el bien jurídico protegido no es la propiedad sino la seguridad de los sistemas que utilizan tecnologías de información se optó por contemplar un tipo especial descriptivo de ese comportamiento.

El artículo 8 contempla la figura culposa de sabotaje o daño a sistemas en virtud del riesgo que supone el uso negligente, imprudente o imperito de tales o del incumplimiento de las normas pautadas para su uso apropiado.

La reprochabilidad de las conductas antes referidas es mayor

cuando recaen sobre un sistema que utilice tecnologías de información o alguno de sus componentes cuando estén protegidos por sistemas de seguridad (artículo 9), situación que se justifica en la mayor audacia del autor.

A la par de la sanción para quien acceda indebidamente, sabotee o dañe sistemas que utilizan tecnologías de información, se tipifica la conducta, cuando está dirigida a realizar o facilitar los daños mencionados, de fabricación, posesión, distribución o venta de equipos destinados a vulnerar o eliminar la seguridad de tales sistemas, o la prestación u oferta de servicios (*hackers)* para sabotaje o daño; de allí la descripción que contempla el artículo 10. Similar previsión pero referida a la posesión, con propósitos delictivos, de equipos para emitir tarjetas inteligentes o instrumentos análogos contempla el artículo 19.

La obtención indebida de datos incorporados en los sistemas que utilicen tecnologías de información o cualquiera de sus componentes, constituye el delito de espionaje informático (artículo 11). En estos casos, con la obtención indebida de bases de datos, por ejemplo, además de haberse vulnerado la seguridad del sistema, resulta comprometida la privacidad de las personas aun cuando el propósito haya sido la obtención de la información general para utilizarla comercialmente (envío de publicidad a todas las personas registradas).

La expansión del comercio electrónico es una de las actividades que obliga a incorporar por lo menos un tipo penal descriptivo de la falsificación o eliminación de documentos o la incorporación de alguno a un sistema que utiliza tecnologías de información (artículo 12). Pero también, el acceso a un sistema para alterar registros, calificaciones, credenciales, antecedentes, requiere de tipificación, al margen de la gravedad de los efectos causados y si hubieren implicaciones económicas. En todo caso, de haber beneficios patrimoniales o indeseables efectos jurídicos con ocasión de estos comportamientos, se agrava la pena.

La disposición se aplica por igual cuando los sistemas se

utilicen como objeto (se alteran los datos incorporados al sistema) o como medio (se crean documentos falsos).

El Capítulo II se dedica a describir algunas conductas en las que los sistemas que utilizan tecnologías de información son utilizados como medio para afectar la propiedad.

El artículo 13 contempla el delito de hurto. En este caso es el propio autor, quien a través del acceso a sistemas que utilizan tecnologías de información, saca de la esfera de dominio de la víctima los bienes tangibles (como el dinero en efectivo) o intangibles (tal es el caso de los créditos o de bonos desmaterializados). La norma propuesta exige la concurrencia de un elemento subjetivo del tipo como lo es el ánimo de lucro.

Si bien la descripción típica del hurto presenta algunas similitudes con el de fraude (artículo 14), ambos se diferencian en que en el segundo son las instrucciones falsas o fraudulentas del autor las que, al alterar o modificar la secuencia lógica de los sistemas, dan lugar a que se produzca una operación que no estaba autorizada, con la consecuencia de la obtención de un activo patrimonial en perjuicio ajeno.

El artículo 15 prevé un tipo especial de fraude perpetrado mediante la utilización de una tarjeta inteligente ajena o un instrumento destinado a los mismos fines para la obtención indebida de efectos, bienes o servicios con evasión del pago respectivo.

En los artículos 16 y 17 se sancionan, respectivamente, la creación, grabación, duplicación o eliminación de la data o información contenidas en una tarjeta inteligente o instrumentos análogos y la apropiación de tales instrumentos con el fin de usarlos o transferirlos a un tercero. En ambos casos, se sanciona a quien sin haber tomado parte en el hecho principal, realice cualquier tipo de intermediación con esas tarjetas o las adquiera o reciba. También se sanciona (artículo 18) la conducta de quien, a sabiendas de su procedencia ilícita, provee dinero, efectos, bienes o servicios al portador del instrumento.

El Capítulo III, en desarrollo del mandato constitucional

contemplado en el artículo 60 de la Carta Magna, conforme al cual la ley debe limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos, describe ciertos comportamientos en los que se afecta la privacidad de las personas y de las comunicaciones a través de sistemas que utilizan tecnologías de información.

Las conductas contempladas en los artículos 20 (violación de la privacidad de la data o información de carácter personal) y 22 (revelación indebida de data o información de carácter personal) se diferencian del delito de espionaje informático propuesto en el artículo 11, en que en este último lo que se protege es la seguridad del sistema que contiene la data o información sea o no de carácter personal, mientras que en los dos primeros se tutela la data o información "personales" o sobre las cuales se tenga un interés legítimo.

Por su parte, el artículo 21 resguarda la privacidad de las comunicaciones, garantizada en el artículo 48 de la Constitución, en la medida en que resulte vulnerada por el uso de tecnologías de información. Con esta regulación se actualiza el concepto de correspondencia incluyéndose la intercepción de e-mails o cualquier otro mensaje de datos transmitidos por un sistema de comunicaciones.

Se incluyó la difusión y exhibición de material pornográfico a niños o adolescentes y su utilización con fines exhibicionistas o pornográficos mediante el uso de tecnologías de información (Capítulo IV) dada la ausencia de regulación de tales comportamientos en la Ley Orgánica para la Protección del Niño y del Adolescente.

En el Capítulo V se describen dos comportamientos: El artículo 25 sanciona la reproducción, copia, modificación distribución o divulgación de programas informáticos (*software*) u otras obras del intelecto, hecho éste que en la actualidad genera grandes pérdidas económicas para los propietarios legítimos. Ahora bien, en el documento de Naciones Unidas sobre los tipos de delitos

informáticos se asienta que éste no es un delito de esa naturaleza debido a que el bien jurídico a tutelar es la propiedad intelectual, no obstante, por afectar programas informáticos y aparecer dentro del elenco de comportamientos reconocidos por Naciones Unidas, se estimó pertinente su inclusión en el Proyecto. En razón de que se exige como un elemento subjetivo del tipo el fin de lucro, se propone como un delito contra el orden económico.

Finalmente, y sin perjuicio de la comisión de un delito más grave, en el artículo 26 se sanciona la oferta engañosa de bienes o servicios mediante el uso de tecnologías de información en la medida en que pueda causar algún perjuicio a los consumidores.

La descripción como tipos agravados que se hace en el Capítulo II del Proyecto, en relación con algunas previsiones similares contempladas en el Código Penal y otras leyes, obedece la peligrosidad que reviste el uso de sistemas que utilizan tecnología de información para la comisión de delitos, más aún cuando se trata de una delincuencia de ordinario especializada pues en la mayoría de los casos el autor tiene habilidad en el manejo de medios informáticos, situación que inclusive puede ofrecer ventajas para intentar hacer desaparecer cualquier evidencia del ilícito cometido.

Se incluye en el artículo 31 un supuesto de indemnización civil especial que impone al juez la obligación de ordenar, en la sentencia de condena por alguno de los delitos que cause un perjuicio patrimonial a la víctima, el pago de una suma de dinero que aquél deberá fijar con el auxilio de expertos. Esta previsión, que persigue concretar uno de los objetivos del proceso penal, cual es la reparación del daño causado a la víctima (artículo 30 de la Constitución y 115 del Código Orgánico Procesal Penal) ofrece una respuesta inmediata a quien ha resultado afectado por alguno de esos delitos, al no forzarle al ejercicio de una acción civil a fin de obtener una reparación por el daño causado.

Sistema sancionatorio

En el Título III se contemplan dos circunstancias agravantes genéricas aplicables, en la medida en que su naturaleza lo permita, a algunos de los delitos previstos en el Proyecto. La más severa reprochabilidad del comportamiento obedece a las facilidades de que ha dispuesto el autor a los efectos de la perpetración del hecho, ya sea porque obtuvo ilegítimamente una contraseña que le permitió acceder a un sistema que utiliza tecnologías de información o, porque su oficio, cargo o función le permitió acceder a una información privilegiada que le facilite el uso indebido del sistema.

Por otra parte y, sin perjuicio de lo establecido en el Código Penal, se contemplan una serie de penas accesorias específicas por la comisión de delitos informáticos; tal es el caso de dos penas accesorias tradicionales como el comiso y la inhabilitación para el ejercicio de funciones. En el primer caso se ordena la incautación de todos los instrumentos o dispositivos destinados a vulnerar o eliminar la seguridad de los sistemas que utilizan tecnologías de información o a la fabricación de tarjetas inteligentes o instrumentos análogos y en el segundo, se prevé la inhabilitación para el ejercicio de ciertas funciones cuando el delito se hubiere cometido con abuso de la posición de acceso a la data o información en razón del cargo o función.

En caso de condena por la comisión de los delitos de acceso indebido y sabotaje o daño culposos, además de la sanción privativa de libertad, se prevé la pena de trabajo comunitario.

Si para la comisión del delito el agente se hubiere valido de una persona jurídica dedicada al ramo de las tecnologías de información, se le suspenderá el permiso, registro o autorización para operar o para dirigir y representar a la persona jurídica.

Además de las sanciones principales y accesorias que el hecho mereciere, se prevé que el tribunal pueda, por cualquier medio, disponer la publicación o difusión de la sentencia. Tratándose de

hechos en los que los sistemas que utilizan tecnologías de información han sido objeto del delito o utilizados como medio para su perpetración, el juez podría ordenar la difusión de fallo a través de alguno de esos sistemas.

Ley contra delitos informáticos

Título I
Disposiciones Generales

Artículo 1.– Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2.– Definiciones. A los efectos de la presente ley, se entiende por:

a.Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del «hardware», «firmware», «software», cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b.Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c.Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d.Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e.Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f.Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g.Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h.Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de *hardware.*

i.Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j.Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k.Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l.Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m.Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n.Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

ñ.Contraseña (*password):* secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

o.Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3.– Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4.– Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las

circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley.

Artículo 5.– Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Título II
De los delitos

Capítulo I
De los delitos contra los sistemas que utilizan tecnologías de información

Artículo 6.– Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7.– Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8.– Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9.– Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de uso restringido sobre personas o grupos de personas naturales o jurídicas.

Artículo 10.– Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11.– Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de

las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12.– Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II
De los delitos contra la propiedad

Artículo 13.– Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14.– Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15.– Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.– Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17.– Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18.– Provisión indebida de bienes o servicios. El que, a sabiendas de que una tarjeta inteligente o instrumento

destinado a los mismos fines, han sido falsificados, alterados, se encuentran vencidos o revocados o han sido indebidamente obtenidos o retenidos, provea a quien los presente, de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19.– Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III
De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20.– Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21.– Violación de la privacidad de las comunicaciones. Incurrirá en la pena de dos a seis años de prisión y

multa de doscientas a seiscientas unidades tributarias, el que, mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajenos.

Artículo 22.– Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV
De los delitos contra niños o adolescentes

Artículo 23.– Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24.– Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V
De los delitos contra el orden económico

Artículo 25.– Apropiación de propiedad intelectual. El que, sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un *software* u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26.– Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III
Disposiciones comunes

Artículo 27.– Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1° Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

2° Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 28.– Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será unicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29.– Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes:

1° El decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.

2° El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3° La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4° La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30.– Divulgación de la sentencia condenatoria. El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31.– Indemnización Civil Especial. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos.

Título IV
Disposiciones Finales

Artículo 32.– Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Artículo 33.– Derogatoria. Se deroga cualquier disposición que colida con la presente Ley.

EPILOGO

Los retos del Estado en el ciberespacio

"...el futuro no es algo que haya que predecir,
sino algo que hay que alcanzar"
Don Tapscott

No existe hoy en día fenómeno que plantee retos más contundentes al Estado que la emergente sociedad digital. Decir aquí que la institución pública se ha visto sobrepasada por el cambio digital es algo que no necesita demostración. Nada más hay que mirar alrededor: mientras la información digitalizada se convierte en el bien más apreciado e intercambiado en el planeta; mientras la digitalización introduce profundos cambios en el funcionamiento de las empresas y de los mercados globales, mientras en las escuelas los maestros se ven cuestionados por un sector de alumnos cada día más informados; mientras más gente se relaciona vía e-mail, o en abarrotados canales de conversación con extraños y lejanos dialogantes, gente a la que nunca ha visto y quizá no verá; mientras todo esto sucede a la vista de todos, el Estado democrático sigue ahí, entre atónito y sorprendido. Sin capacidad para responder a la vertiginosa velocidad del cambio.

El Estado y la propia autoridad política se ven en apuros. Las redes permiten a la sociedad en cierta forma escapar a los controles públicos, algo que todos en algún momento queremos hacer; la fiebre por conectarse se enfrenta a la miseria espiritual de millones de internautas aislados de su realidad inmediata; el equilibrio o desequilibrio entre la cantidad y la calidad de la información plantea enormes problemas sobre las bondades de la información ilimitada; el choque entre la supuesta libertad que nos dan las redes y el control cada vez más férreo sobre nuestros actos por parte de los sistemas informáticos (y sus dueños); las amenazas cada vez más fuertes de los delincuentes sin rostro, las mafias y la delincuencia organizada; el auge de la pornografía, la mercantilización y la destrucción de los valores

democráticos, forman, entre otros, problemas con los que tendrá que lidiar el Estado y la sociedad en los próximos años.

Como hemos visto, en muchos países la respuesta ha comenzado mediante la adopción de una legislación que intenta responder a los novedosos fenómenos del ciberespacio. Este es un paso vital. Siendo el Estado el responsable de velar por el espacio público, es lógico esperar que se busque crear un marco regulatorio, de normas y principios, capaz de servir como sistema de referencia para delimitar lo aceptable de lo inaceptable, lo legal de lo ilegal, lo deseable de lo indeseable y que, en suma, trate de evitar que los costos y perjuicios aparejados al cambio digital sean mayores que los beneficios y avances para la sociedad y el individuo.

Una de las conclusiones de este proceso ha sido sin duda la necesidad de crear referencias legislativas locales, y posteriormente armonizar dichas leyes nacionales con acuerdos internacionales, instrumentos necesarios para responder a fenómenos como la extraterritorialidad de lo digital. Pero para que tales acuerdos sean posibles es necesario, en primer lugar, contar con leyes en cada uno de nuestros países. Leyes modernas y flexibles que brinden un primer marco de actuación a las instituciones públicas, a los gobiernos y a los ciudadanos. Los delitos teleinformáticos, por su extensión, proliferación y nocivos efectos deben constituir, dentro de este esquema, un punto prioritario de atención.

En América Latina, como hemos dicho anteriormente, la tendencia a establecer legislaciones especiales que atiendan los fenómenos digitales comenzó apenas en la década pasada. En Venezuela, recién en los últimos tres o cuatro años se ha despertado el interés por regular actividades de comunicaciones y procesos teleinformáticos, mientras se han dictado medidas ejecutivas y decretos dirigidos también a suplir algunas de las frecuentes lagunas con que nos enfrentamos como sociedad al cambio digital. Venezuela se encuentra hoy sin duda en el camino de modernizar toda su legislación para adaptarla a las exigencias de los nuevos procesos que transforman la economía y la sociedad mundial.

En este contexto, el proyecto de Ley contra delitos informáticos que acompaña este libro busca servir de herramienta en la compleja tarea de construir un conjunto de políticas públicas para abordar estos problemas y fenómenos. Desde la óptica estrictamente legislativa suscribimos plenamente la posición sostenida por la mayoría de los especialistas respecto a la necesidad de reformar a fondo el Código Penal venezolano, un instrumento que data de principios de siglo y que está exigiendo una urgente adaptación a los nuevos tiempos. La ley de delitos informáticos que presentamos en esta propuesta se inscribe pues dentro de la necesidad de dictar instrumentos legislativos que sirvan de soporte y den respuesta a una urgente necesidad social, mientras se realiza la tarea de reingeniería legislativa necesaria para modernizar la legislación penal venezolana.

Sabemos que legislar es necesario pero no suficiente. Una Ley y un Código Penal modernos y flexibles son imprescindibles pero insuficientes porque los efectos de la digitalización se ejercen sobre toda la sociedad, sobre todos los actores y en todo momento. Es por ello que tareas y proyectos como dar acceso a los ciudadanos de forma responsable y equitativa, y enfrentar el peligro de la llamada brecha digital que amenaza con dividir más a la sociedad entre conectados y desconectados, se convierten en acciones de políticas públicas de la más alta prioridad. En este sentido, vemos emerger en Venezuela una renovada conciencia dentro del sector público acerca de la urgente necesidad de brindarle a nuestros ciudadanos, y en particular a los sectores más desfavorecidos, la oportunidad de acceder a las herramientas del conocimiento.

Pero el acceso por sí solo tampoco basta. Resulta impostergable capacitar técnicamente a los ciudadanos, funcionarios y trabajadores en torno al uso y aprovechamiento de las tecnologías digitales. La idea de que el gobierno puede efectivamente no sólo regular sino participar activamente en los procesos digitales, es definida hoy como la de un Gobierno Electrónico. Esta tesis sostiene que los Estados pueden y, sobre todo deben si quieren sobrevivir en la sociedad del conocimiento, reinventar su rol mediante el

aprovechamiento de las nuevas herramientas telemáticas.

La elevación de la calidad en servicios como educación, capacitación, salud, atención social, sistemas de información, recaudación de impuestos, cooperación, control presupuestario y de gestión, y participación (lo que algunos llaman teledemocracia) entre otros, constituyen áreas en las que el Estado está obligado a ser más eficiente y más efectivo. Reducirse a su rol regulador no bastará si no se convierte también en actor y catalizador del proceso.

Vemos también prioritario difundir una ética de responsabilidad social en torno al uso de los nuevos medios de comunicación e información digitales. No bastará la ley ni la buena disposición de maestros, jueces, funcionarios públicos e instituciones en general si no incorporamos la dimensión ética al manejo de estos medios y herramientas. El manejo de la información se convierte en la sociedad global en una responsabilidad colectiva.

Como ninguna otra sociedad en la historia, tenemos hoy la posibilidad extraordinaria de acceder y manejar cantidades ilimitadas de información. Esto de por sí conlleva una enorme responsabilidad y no sólo para el Estado, garante del equilibrio y la equidad social, sino también de cada ciudadano, cada familia y cada empresa. Fortalecer las actitudes y valores que promuevan el respeto, la diversidad, la tolerancia, la cooperación, la solidaridad, el trabajo y la paz se convierte así en un objetivo impostergable.

El reciente proceso de apertura de las telecomunicaciones en nuestro país, constituye el eje de este proceso. Gracias a este proceso, los venezolanos nos veremos progresivamente con una mayor oferta de servicios de comunicación e información. La ampliación de este mercado conllevará por sí solo a una diseminación de la cultura digital y, junto a los beneficios económicos y sociales, se agravarán las amenazas y los peligros, particularmente en la forma de delitos informáticos. Es responsabilidad indecli-nable del Estado prepararse y alertar a los ciudadanos sobre ello.

Se trata pues de enormes tareas y complejos retos. Asumir estos desafíos, respetando los principios democráticos y fortaleciéndolos,

constituye un proyecto extraordinario en un país que recién comienza el camino de la construcción de nuevas instituciones.

Este libro pretende ser un aporte a este proceso. Como justamente afirma Jacques Le Goff, «no se trata de reducir a unidad la diversidad, sino de lograr una diversidad convergente». En los próximos años, se necesitará mucha imaginación, voluntad política y sensatez del lado del sector público para enfrentar las dimensiones e insospechadas repercusiones del cambio digital.

La problemática de la inseguridad virtual pasará a ser tema prioritario en la agenda pública. Enfrentar y derrotar a los delincuentes que se valen de los medios digitales y telemáticos será con el tiempo una exigencia mucho más firme de la sociedad y los ciudadanos. La amenaza a la vida individual, social y económica es demasiado grande para ser ignorada.

Sabemos que la sociedad digital puede ser una increíble herramienta para promover la igualdad de oportunidades, el desarrollo espiritual y económico de las personas y la riqueza social, pero debemos velar porque este proceso no liquide la pluralidad y se convierta en una nueva arma de dominación entre quienes manejan y dominan la tecnología y quienes no pueden acceder a ella. Cuando se trata de información, combinar libertad y responsabilidad es aún más importante que en cualquier otro aspecto.

Gracias al fenómeno de la información hoy el ser humano vuelve a ser el centro de discusión filosófica en el mundo. Después de todo, no son los modelos teóricos de sociedades idealizadas del pasado o del futuro, lo que nos sacará de los problemas. Será la calidad de nosotros mismos, la capacidad de nuestra gente, el talento, la educación, la imaginación, la innovación. Gracias a la información volvemos a retomar nuestro rol central como sujetos de nuestra propia superación. Ninguna cadena nos atará más que nuestra propia capacidad para romperla.

Si este texto y esta propuesta legal contribuyen a elevar el grado de información, la conciencia pública y la necesidad de la acción responsable y colectiva, sentiremos que hemos dado un aporte positivo

a la tarea de construir un nuevo tipo de desarrollo. Un desarrollo equitativo, sostenible, justo y democrático. Un desafío que sólo aguarda por nosotros.

ANEXO I

Glosario

Nota de los editores: El siguiente glosario contiene un conjunto de términos ligados a la temática debatida en este libro. Se trata de una recopilación basada en criterios de comprensión y comunicación y no aspira por tanto al rigor técnico que requiere una publicación especializada. Se ofrece como complemento y apoyo al lector interesado.

Antivirus: Programa que busca, detecta y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, diskette u otro soporte.

Aplicaciones de negación de servicio: Estos programas o recursos permiten dejar colgado o desactivar un servicio de la red saturándolo de información y bloqueándolo, e incluso obligando a reiniciar la máquina.

Ataques asincrónicos: Es uno de los procedimientos más complicados de saboteo. Periódicamente se graban determinados datos en un sistema, y si alguien logra que el sistema se caiga o se paralice, es posible entonces modificar determinados archivos, de manera que cuando se pone de nuevo en funcionamiento el sistema, éste operará con la nueva información, provocando alteraciones o errores.

Backup(copia de respaldo, copia de seguridad): Es una medida de precaución para el cuidado de la información que consiste en crear un respaldo o copia de seguridad, de tal manera que si por una u otra razón se borra o echa a perder el original, podremos utilizar la copia.

Nos evitará problemas el tener siempre una copia de nuestro trabajo.

Base de datos: Conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.

Bit (*bit*, bitio): Se trata de la unidad mínima de información que se maneja en una computadora. Se deriva de la contracción de la expresión *binary digit* (dígito binario).

Bug (error, insecto, *bicho*): Se remonta este concepto informático al año 1945 cuando la ingeniera Grace Murray, valuarte en el desarrollo de la programación moderna, notó cómo un insecto (*bug*) había echado a perder uno de los circuitos de una computadora en la que trabajaba.

Caballo de Troya: Esta técnica consiste en introducir dentro de un programa una *rutina* (conjunto de instrucciones que realizan una tarea) no autorizada y desconocida por la persona que lo ejecuta, para que dicho programa actúe de una forma diferente a como estaba previsto; el creador del programa tiene la oportunidad de accesar al interior del sistema que lo procesa. De esa forma se logra por ejemplo, modificar un fichero o grupo de archivos, extraer mensajes, obtener información privilegiada del sistema, etc. Es uno de los recursos de piratería más populares.

Cazador de contraseñas: Este programa intenta *desencriptar* o descodificar las claves o contraseñas (password) de un sistema de información y eliminar la protección que aquéllas le brindan. Una vez desencriptada la clave se consigue el acceso al sistema de datos y por ende se puede fácilmente manipular y usar la información.

Chat(conversación, *charla*, chateo, platicar): Servicio ofrecido en Internet mediante el cual las personas pueden conversar en salas o canales de conversación en línea mediante el envío y recepción de textos. Es el servicio más popular entre los jóvenes. La expresión

"chatear" ya indica una actitud cultural, la permanente conversación en Internet con amigos o desconocidos. Existen diversas plataformas y programas que se utilizan para chats. Los más vanguardistas permiten ya la transferencia de audio y video en tiempo real.

Chip (microprocesador): La parte más importante de una computadora la representa este circuito con soporte de silicio e integrado por transistores y otros componentes electrónicos. Es el cerebro de los computadores.

Ciberespacio: Fue utilizado por vez primera en la novela «Neuromancer» de William Gibson en donde se aplicaba para describir un universo de computadoras y una civilización creada en torno a estas máquinas. Lugar indefinido, donde los seres humanos se encuentran y comunican a través de la red. Aunque no es exactamente «real», es un lugar que existe. Hay cosas que ocurren allí que tienen consecuencias muy reales.

Cibernauta(Cybernaut o Internauta): Usuario que navega por la red.

Clonación (de tarjetas): Procedimiento mediante el cual se captura digitalmente la información de seguridad contenida en una tarjeta electrónica y luego se reproduce una copia ilegal de la misma, que es usada con fines de defraudación.

Cyberpunk (*descifrador de claves*, resuelve cifras): Es por lo general un especialista informático de alta capacidad cuya función primordial es la de romper las claves criptográficas y superar los sistemas de seguridad por sofisticados que sean. Persona especializada en romper claves criptográficas y superar sistemas de seguridad.

Cookie (cuqui, espía, delator, fisgón, galletita, pastelito): se trata de un conjunto de programas, en ocasiones encriptados en el mismo navegador, que se almacenan en el disco duro de la computadora del

usuario cuando éste entra a determinadas páginas en Internet. Numerosas protestas se han originado respecto al tema, ya que en muchas ocasiones las compañías utilizan esto para conocer las preferencias de los usuarios y de esta manera enfilar una campaña publicitaria.

Cracker (intruso, saboteador): Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad. Son personas muy capaces y que cuentan con una serie de herramientas para lograr su cometido. Se tiende a diferenciar del Hacker en la intención.

Criptografía (cryptos grafos): Arte o ciencia de la escritura secreta. Procura ocultar los mensajes o información de ojos ajenos. Consiste en cifrar y descifrar mensajes. En computación se refiere a los mensajes que son enviados por un emisor que oculta el contenido del mensaje a manera de que sólo ciertas personas tendrán acceso a la información por medio de una clave. Resuelve los siguientes problemas: Privacidad, Autenticidad,No rechazo, Integridad.

Data (datos): Plural de la palabra latina *datum* (dato). Puede caerse en el error al emplearse en inglés y pensar que se refiere a un solo dato.

Desencriptar: Descodificación o revelación de códigos de seguridad.

Destinatario: Persona, natural o jurídica a quien va dirigido el Mensaje de Datos.

E-commerce (Comercio electrónico):Cualquier forma de transacción o intercambio de comercial basada en la transmisión de datos que utilizan la tecnología de la información y las comunicaciones. Puede hablarse de comercio electrónico cuando todo el proceso de negociación y compra venta de productos y servicios se realiza mediante sistemas teleinformáticos.

Emisor: Persona, natural o jurídica, pública o privada, que origina un mensaje de datos por sí mismo, o a través de terceros autorizados.

Encriptar: Proceso general de codificación de datos con un propósito de seguridad.

Encriptación (encryption, cifrado)*:* Se trata de un mecanismo de seguridad en Internet cuya principal función es la de hacer llegar la información a un determinado usuario sin que nadie más pueda tener acceso a ella. Existen diversos tipos de cifrados que en cierta manera son la base de la seguridad de la red.

Firewall (barrera contra fuegos)*:* Se denomina así al sistema de seguridad que se coloca entre la red local e Internet, de esta manera la empresa o compañía regulará completamente toda la comunicación hacia Internet estableciendo sus políticas de seguridad. En ocasiones este sistema incorpora autentificación de usuarios entre otras cosas.

Firma electrónica: Información creada o utilizada por el signatario, asociado al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido utilizado.

Gusanos: Se fabrica de forma análoga al virus con miras a infiltrarlos en programas legítimos de procesamiento de datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor, benigno, mientras que el virus, un tumor maligno. Pero 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. Es un virus que suele llegar a través del correo electrónico, en forma de archivo adjunto. En 1998 tuvo por vez primera aparición uno de estos programas que afectó a más de 6.000 sistemas en Internet.

Hacker (pirata): Persona con destrezas y conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer, este término no debe de llevarse al extremo de alguien malo con fines de destruir sistemas, esto encaja mejor en la definición de «cracker». Suelen ser jóvenes deseosos de conocer el funcionamiento de los diferentes sistemas. El Hacker aprovecha los agujeros, los fallos de los sistemas de seguridad. Sus intereses se centran en el conocimiento del funcionamiento de los sistemas. Acceden de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse del autor.

Hacking: Actividad del hacker.

Hardware (fierros, maquinaria): Se trata de todos los componentes físicos de una computadora, entre los cuales se pueden mencionar el disco duro, procesador, monitor, etc. que en conjunto con el software (programas) hacen que funcione nuestra máquina.

Herramientas de destrucción: Programas o rutinas programadas para que en una fecha determinada modifiquen la información contenida en un sistema, o provoquen fallos en éste. Algunos ejemplos son:

- *Flash bombs,* pueden expulsar a otros usuarios de un servicio de conversación en línea o chat, dejar colgado el chat, o llenar de basura (mensajes sin sentido, textos largos, etc.) un determinado canal de conversación.
- *Mailbombing,* consiste en enviar miles de mensajes de correo electrónico al mismo usuario, lo cual provoca una gran molestia. Esta técnica ha sido usada durante los últimos años en ataques contra algunos de los sitios más populares de Internet (yahoo.com, cnn.com, amazon.com, ebay.com, entre otros), logrando en algunos casos que

la sobrecarga de mensajes de correo (mails) sature los sistemas y servidores de dichas empresas, hasta paralizar las operaciones por cierto tiempo.

Internet (La Red): Se denomina así a la red de telecomunicaciones que surgió en los Estados Unidos en 1969 por el Departamento de Defensa de los Estados Unidos, más precisamente. Se la llamó primero ARPAnet y fue pensada para cumplir funciones de carácter meramente militar, para convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en diversos aspectos como son el social, cultural, económico, etc. Internet es además una red multiprotocolo capaz de soportar cualquier tecnología. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

*Internet*2: Proyecto de interconexión de más de cien universidades estadounidenses. El objetivo es desarrollar una red de altísima velocidad para la educación y la investigación.

Intranet: Red de redes de una empresa o institución. Se le conoce como la Internet interna de una organización.

Junk mail (correo basura): Publicidad masiva y no solicitada, a través del correo electrónico. Se la considera una práctica comercial poco ética, opuesta a las reglas de netiquette.

Malware (malgrama(s) programa(s) maligno(s), software maligno): Se trata de cualquier tipo de software que tiene como meta el causar un daño o perjuicio, ya sea a una computadora o a una red.

Mensaje de datos: Toda información, inteligible o encriptada, en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

On line: (en línea, conectado): Estado en que se encuentra una computadora cuando se conecta directamente con la red, a través de un dispositivo, por ejemplo, un \l «modem» módem.

Página web: Una de las páginas, archivos o documentos que componen un sitio de la World Wide Web. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se la llama «home page».

Password (contraseña): Secuencia alfabética, numérica o combinación de ambas (alfanumérica), protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

Phracker (fonopirata): Es un individuo de alta capacidad en el manejo y manipulación de las redes telefónicas, las cuales utiliza para obtener cierta información de redes ajenas. En muchas ocasiones se pone en juego este tipo de prácticas para evadir el pago de los recibos telefónicos. Acceden a la red utilizando «vías» gratuitas de las que disfrutan ilícitamente o de forma no autorizada.

Puertas falsas: Se crean cuando los programadores introducen interrupciones en la lógica de los programas para chequear la ejecución de éstos, con el objetivo de producir y corregir determinados errores; pero, después de chequeado el programa, cuando el programa se le entrega al usuario, esas rutinas no se eliminan, y son aprovechadas por los hackers o crackers para acceder al sistema.

Realidad virtual: Simulación de un medio ambiente real o imaginario que se puede experimentar visualmente en tres dimensiones. La realidad virtual puede además proporcionar una experiencia interactiva de percepción táctil, sonora y de movimiento.

Recogida de basura electrónica: Consiste en aprovechar la información

que queda abandonada en forma de residuo. Se explora la zona de memoria o zonas del disco en las que queda información residual que no fue realmente borrada y que puede ser usada posteriormente.

Red: En tecnología de la información, una red es un conjunto de dos o más computadoras o recursos interconectados.

Signatario: Es la persona, natural o jurídica, pública o privada, titular de una firma electrónica o certificado electrónico.

Simulación de identidad: Consiste en usar un terminal de un sistema en nombre de otro usuario, ya sea porque se conoce su clave, o porque de alguna forma se tuvo acceso al terminal de forma no autorizada. El término también es aplicable al uso de tarjetas de crédito o documentos falsos en nombre de otra persona. Este método es utilizado frecuentemente para cometer fraude y otros delitos mediante el uso de información adquirida ilícitamente de otras personas en la red, e identifica claramente los peligros que deben encarar quienes hacen negocios por Internet.

Sistema de Información: Aquel utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma Mensajes de Datos.

Sniffer: Es un recurso o proceso que captura la información que viaja a través de una red, para ser analizados posteriormente, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de paquetes de datos, que se intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante; el sniffer está diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad. Un ataque de este tipo se considera de un alto riesgo, porque además de capturar contraseñas, se pueden obtener números de tarjetas de crédito, información confidencial y privada, etc. Actualmente existen sniffers para todas las plataformas, ya que los sniffers se dedican a capturar datos, no

computadoras, y por ello es igual la plataforma que se utilice. Los sniffers no se pueden detectar, ya que son aplicaciones pasivas que no generan nada, por lo que no dejan ningún tipo de huella. Son especialmente indetectables en DOS y Windows 95, y trabajo en grupo, aunque en UNIX y Windows NT haya más posibilidades de detectarlo.

Software: Término general que designa los diversos tipos de programas usados en computación.

Spam: (bombardeo publicitario, buzonfia): Los odiados spams no son más que los envíos masivos e indiscriminados de publicidad a través de correo electrónico no grato para el destinatario.

Spoofing: Permite que se utilice una máquina con la identidad de otra persona; o sea, se puede acceder a un servidor remoto sin utilizar ninguna contraseña; para ello, el hacker se apropia de la dirección de otro usuario, y así hacen creer al servidor que se trata de un usuario autorizado.

Superzapping: (Zap, borrar): Comando que usualmente borra los datos dentro de un archivo pero deja intacta la estructura del archivo, de tal manera que puedan introducirse nuevos datos. Es el uso de un programa editor de ficheros (archivos) para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de una computadora. El nombre proviene de una utilidad llamada SUPERZAP que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serían las Pctools o el Norton Disk Editor.

Telemática: (Teleinformática). Combinación de las palabras «telecomunicaciones» e «informática». Disciplina que asocia las telecomunicaciones con los recursos de la informática.

Telnet: Se refiere a un protocolo estandarizado en Internet que se utiliza para realizar la conexión desde una terminal remota. En la

actualidad casi en desuso.

Virus: Se le llama así a todo programa computacional que se duplica a sí mismo dentro de un sistema y que se añade a otros programas que se utilizan ocasionando fallas. En la actualidad son la principal preocupación de los usuarios que navegan en Internet, en donde tienen su mayor campo de acción; puede causar efectos indeseables y hasta daños irreparables.

Website(sitio web, servidor web): Es una serie o colección de páginas de Internet que tienen una sola dirección. Es un lugar de información, ya sea un directorio, un portal, una tienda virtual o cualquier otro punto de la red donde el usuario que interactúa puede realizar diferentes actividades.

World Wide Web(www, W3): Red mundial, sistema global de la información basado en la tecnología del hipertexto, que se crea en los 90´s por Tim Berners Lee, investigador en el CERN, Suiza. Este sistema soporta todo tipo de información (audio, video, imagen, texto, etc.) y se accesa de manera fácil por los usuarios a través de los navegadores.

ANEXO II

Directorio y referencias

Entregamos aquí un pequeño directorio de las instituciones, empresas y organizaciones vinculadas al área de los delitos informáticos en Venezuela, así como direcciones electrónicas donde el lector podrá ampliar información al respecto. Estas direcciones y datos han sido recolectados en distintas fuentes por lo cual no se garantiza su actualización ni fiabilidad.

PODER LEGISLATIVO NACIONAL

Asamblea Nacional de Venezuela
http://www.asambleanacional.gov.ve

Asamblea Nacional de Venezuela
Sub Comisión de Fraudes Informáticos:

Dip. Carlos Tablante
ctablante.an@platino.gov.ve

Dip. Norberto Peña
npena.an@platino.gov.ve

Dip. Elías Matta
ematta.an@platino.gov.ve

PODER EJECUTIVO NACIONAL

Ministerio de Ciencia y Tecnología
http://www.mct.gov.ve

Instituto para la Educación y Defensa del Consumidor (INDECU)
http://www.indecu.gov.ve

Centro Nacional de Tecnología de la Información-CNTI.
http://www.reacciun.ve

Cuerpo Técnico de Policía Judicial- CTPJ
http://www.ctpj.gov.ve/

PODER JUDICIAL NACIONAL

Tribunal Supremo de Justicia
http://www.tsj.gov.ve

SECTOR PRIVADO

Cámara Venezolano-Americana de Comercio e Industria-Venamcham.
http://www.venamcham.org/

Cavedatos
http://www.cavedatos.org

ORGANISMOS PUBLICOS INTERNACIONALES

Computer Crime Squad - FBI. Buró Federal de Investigaciones del Gobierno de los Estados Unidos de América.
http://www.tscm.com/compcrim

Cooperación Internacional en Tecnologías Avanzadas (CITA)
http://www.cita.es

ORGANISMOS PRIVADOS INTERNACIONALES

BSA Venezuela
http://www.bsa.com.ve

BSA España
http://www.onnet.es/bsa

BSA Estados Unidos
http://www.bsa.org

INSTITUCIONES GREMIALES DEL SECTOR PRIVADO

Asociación Bancaria de Venezuela
http://www.asobanca.com.ve
Ignacio Salvatierra- Presidente (Unibanca).

Cámara Venezolana de Tarjetas de Crédito y Afines.
Kumar Rao- Presidente (American Express, Corp Banca).
cvtc@gr3000.com

SITIOS EN INTERNET

http://www.bufetalmeida.com/
Especialistas en delitos informáticos; Internet y responsabilidad civil.

http://mansci1.uwaterloo.ca/~msci604/604_95w9.html
Prevención de delitos
eiriarte@corp.vlex.com
REDI (Revista Electrónica de Derecho Informático).

http://www.abogadoconsulta.com
Consultas sobre delito informático en Chile.

http://www.veraz.com
Información sobre fraude informático.

http://www.first.org
FIRST

SISTEMA FINANCIERO VENEZOLANO

BANCA UNIVERSAL

ABN-AMRO BANK
Sr. Esven Bax. Presidente
Centro Seguros Sud América, piso 1. Av. Francisco de Miranda.
El Rosal.
Tlf. 957.03.56 - 957.03.00. Fax. 953.57.58

BANESCO
Dr. Xavier Luján. Presidente Ejecutivo.
Av. principal de Las Mercedes con calle Guaicaipuro Edif. Banesco.
El Rosal
Caracas. Tlf. 901.84.01/901.82.84/86.01. Fax. 901.89.98

BOLÍVAR BANCO UNIVERSAL, C.A
Dr. Benardo Velutini. Presidente.
Centro Lido, Torre C, piso 10, Of., 100C.
Caracas
Tlf. 957.93.02/03/04. Fax. 957.94.02
Sr. Rubén Idler. Vicepresidente.
Edif. Banco Caracas, Veroes a Santa Capilla, Av. Urdaneta,
Caracas. Tlf. (D): 505.17.58/59. Fax: 864.65.53

CORP BANCA C.A. BANCO UNIVERSAL
Dr. Lautaro Aguilar. Presidente Ejecutivo.
Torre Corp Banca. Planta C. Edif. Anexo.
Av. Principal La Castellana,
entre Av. Blandín y Los Chaguaramos. Caracas.
Tlf. D.206.32.29 C. 206.33.33. Fax. 206.32.14

DEL CARIBE C.A. BANCO UNIVERSAL
Dr. Edgar A. Dao. Presidente.
Dr. Paúl a Salvador de León. Tlf. 505.51.03. Fax: 562.04.60
eadao@bancaribe.com.ve

DEL CARONI
Dr. Arìstides Maza Tirado. Presidente.
Av. Universidad Esq. Monroy, Planta Baja,
Caracas.
Tlf. 509.51.66/67/509.52.00 - (086) 221835
Fax. 577.87.57

CITIBANK
Sr. Philip Henriquez. Presidente.
Carmelitas a Altagracia. Caracas.
Tlf. (D) 806.23.37/ 819501/5490/825987 Fax: 860.64.93
elizabeth.alexander@citicorp.com

VENEZUELA
Sr. Michel Goguikian. Presidente Ejecutivo.
Av. Universidad, Sociedad a Traposos Torre Banco de Venezuela.
Caracas.
Tlf. (D) = 501.25.56/501.25.21/22/23. Fax. 501.25.70
mjgoguikian.caracas@sinvest.es

EXTERIOR, BANCO UNIVERSAL
Dr. Sergio Sannia. Presidente Ejecutivo
Av. Urdaneta, Esq. Urapal, Caracas.
Tlf. 501.01.41/42/43 501.01.11
Fax. 73.37.98/501.07.49

MERCANTIL
Dr. Gustavo A. Marturet. Presidente.
Edif. Mercantil, piso 19, Av. Andrés Bello. Caracas.
Tlf. 507.71.11/11.12/11.1. Fax. 575.14.61/19.80
ygalea@bancomercantil.com

BBVA PROVINCIAL
Sr. José Carlos Pla. Presidente.
Centro Financiero Provincial, piso 8, Av. Volmer, San Bernardino.
Caracas.
Tlf. (D) 504.43.34/574.85.22/576.46.11. Fax. 574.17.65
ana_zapata@www.pidanet.com

CONFEDERADO
Dr. Hassan Saleh. Presidente.
Avda. Universidad, de Traposos a Chorro. Esquina Pasaje Linares. Caracas.
Tlf. 542.25.34 - 542.14.66 - 542.06.68. Fax. 542.02.82/542.07.89

FONDO COMUN, BANCO UNIVERSAL
Dr. Fortunato Benacerraf. Presidente Ejecutivo.
Torre Fondo Común. Avenida Andrés Bello. Caracas.
Tlf. 597.21.01/02. Fax. 597.21.10

UNIBANCA, BANCO UNIVERSAL
Dr. Juan Carlos Escotet. Presidente Ejecutivo.
Av. Universidad, Esquina El Chorro. Caracas.
Tlf. (D)= 501.70.33/33/501.71.11/70.21
Fax. 501.73.42/561.55.41
jescotet@banesco.com

UNIBANCA, BANCO UNIVERSAL
Dr. Ignacio Salvatierra. Presidente Junta Directiva.
Av. Universidad, Esquina El Chorro. Caracas.
Tlf. (D) 501.70.33/33/501.71.11/70.21
Fax. 501.73.42/561.55.41
ignacio_salvatierra@bancunion.com

NORVAL BANK C.A., BANCO UNIVERSAL
Dr. Fernando Dávila. Presidente Ejecutivo.
2a. Av. Campo Alegre. Torre Cari. P.H. 1, Campo Alegre. Caracas.
Tlf. 953.48.44/18.62/42.55/10.43. Fax.953.28.43
gmacha@noroco.com

BANCA COMERCIAL DE VENEZUELA

CANARIAS DE VENEZUELA
Dr. Manuel Herrera Castilla. Presidente.
Torre Financiera Canarias, Boulevard de Sabana Grande. Caracas.
Tlf. 706.91.00. (D) 706.91.10/91.13/91.05
Fax: 706.91.21

CHASE MANHATTAN BANK VENEZUELA, C.A
Sra. Marianela Hernández. Presidenta.
Centro Cremerca, P.H.. Avenida Venezuela, El Rosal. Caracas
Tlf. 901.05.11/0580/0647/5533

BANCO DE CORO C.A. (BANFOCORO)
Dr. Abraham Senior Urbina. Presidente.
Av. San Juan Bosco con Av.. Francisco de Miranda. Edif. Adriática de Seguros, P.B.
Tlf. Caracas: 263.31.81 - 263.45.02 - 263.23.92
Tlf. Coro: (068) 51.03.32/51.45.32/51.67.98 24.54/51.12.87/ 52.11.78. Fax. /068) 51.16.90/51.98.14/52.11

DE FOMENTO REGIONAL LOS ANDES
Lic.Edgar A. Hernández B.. Presidente
Edf. Polar, Planta Baja, Letra PB-K. Urb. Los Caobos, Plaza Venezuela. Caracas.
Tlf. (076)46.63.16/47.47.31/47.60.97/59.55/44.97.84
Fax. (076) 466316/44.97.84

DE COMERCIO EXTERIOR (BANCOEX)
Dra. Lieber Patiño. Presidenta.
Centro Gerencial Mohedano, calle Los Chaguaramos, P.H. Este La Castellana. Caracas.
Tlf. 265.14.33. Fax: 265.67.22

DO BRASIL
Sr. Elmo Pahl. Gerente General.
Av. Francisco de Miranda, Edif. Centro Lido, Piso 5,Ofc. 51-B, El Rosal, Caracas.
Tlf. 952.26.74. Fax. 952.35.95/952.52.51

BANCO STANDARD CHARTERED
Sr. Carlos Rojas. Gerente General.
Av. La Estancia, Centro Banaven. (Cubo Negro), Núcleo "D", piso 5. Urb. Chuao.
Tlf. 993.32.93 991.39.58 – 992.07.21. Fax: 992.26.49 993.42.69

EUROBANCO
Sr. Alejandro Pizzorni. Presidente.
Calle Paris, entre New York y Trinidad, Torre Eurobanco, Las Mercedes . Caracas.
Tlf. 992.00.45/05.20/05.31. (C-992.63.76-01.67). Fax: 992.59.45

FEDERAL
Dr. Nelson Mezerhane. Presidente.
Centro Cremerca, Av. Venezuela, piso 6, El Rosal, Caracas.
Tlf. (D) 951.53.80/14.12. (C) 901.50.11. Fax. 951.44.49
nmezerhane@banco-federal.com

BANCO DE CREDITO DE COLOMBIA, S.A.
Dr. Fernando Peláez. Gerente General.
Av. Venezuela, El Rosal, Torre Mariana, P.B., Caracas.
Tlf. 952.88.41/35.15. Fax. 952.44.52/952.82.13

GUAYANA
Dr. Oscar Eusebio Giménez. Presidente.
Calle Libertad Nº 1, Ciudad Bolívar-Edo. Bolívar
Tlf.086/65.07.17/18. (085) 22011/014/27146/.
Fax. (086) 65.07.64

INDUSTRIAL DE VENEZUELA
Dr. Fernando Alvarez Paz. Presidente.
Tercera Avenida de Las Delicias de Sabana Grande,
cruce con Avenida Francisco Solano López, Torre Financiera,
Parroquia El Recreo
Caracas.
Tlf. (D) 952.40.51/ 952.39.93 -952.60.84-952.40.04- y 952.41.93
Fax. 952.62.82

ING BANK
Sr. Bert Denkers. Country Manager.
Avenida Eugenio Mendoza (Principal de La Castellana).
Centro Letonia, Torre ING BANK, piso 16. Urb. La Castellana,
Estado Miranda.
Tlf: 263-82-33/263-83-33. Fax: 263-22-66

MONAGAS
Dr. Rafael Gill Ramírez. Presidente Ejecutivo
Banco Caroní.
Presidencia. Av. Universidad, Esq. Monroy. Planta Baja.
Caracas.
Tlf. 953.44.22/42.13/60.55/42.22. Fax. 953.75.78

OCCIDENTAL DE DESCUENTO
Sr. Victor Vargas. Presidente.
Edif. Centuria, Mezzanina, Av.Venezuela con calle Mohedano,
El Rosal
Tlf. 953.86.36/ (D) 952.81.09/952.53.18953.89.05/89.36/89.07/
86.36 - 061/92.45.56/59.52.94. Fax; 952.86.38
cvalentin@bodinternet.com

VENEZOLANO DE CREDITO
Dr. Oscar García Mendoza. Presidente.
Avenida Alameda, Urbanización San Bernardino (antigua torre Norte del conjunto de edificios de la C.A. La Electricidad de Caracas), Tlf. 806.61.11/806.60.00
Fax. 806.65.55

PLAZA
Sr. Agostino De Sousa Macedo. Presidente.
Torre Banco Plaza, P.H. Avda. Casanova. Esq. Calle Villaflor
Tlf. 761.39.68/96.19/761.99.75/91.36/761.97.46

SOFITASA
Dr. Juan A. Galeazzi Contreras. Presidente.
7ma. Av. Esq. Calle 4, Edif. Banco Sofitasa,
San Cristóbal-Edo. Táchira
Tlf. (076) 43.43.55 - 40.45.55. Fax. (076) 44.38.95/43.16.31

TEQUENDAMA
Dra. Marina Alarcón. Representante Legal.
Av. Tamanaco, Edif. Seguros Banguaira P.B. El Rosal. Caracas.
Tlf. 951.21.22/20.09. Fax. 951.20.04
malarcon@btequendama.com.ve

NUEVO MUNDO, BANCO COMERCIAL
Dr. Luis Eduardo Correa. Presidente.
Avenida Luis Roche con 3ra. Transv. Altamira, Torre Nuevo Mundo, Chacao.
Tlf: 201.18.07 – 201-18.00 – 201.18.11.
Fax: 201.18.09 – 201.18.10- 201.18.88

TOTALBANK C.A., BANCO COMERCIAL
Dr. Victor Gill Ramirez. Presidente.
Avenida Pichincha con calle Guaicaipuro, Torre Alianza, piso 9.
Urb. El Rosal, Caracas.
Tlf. 953.44.22/42.13.60.55/42.22/59.33/49.33/59.79
Fax: 953.75.78

TOTALBANK C.A., BANCO COMERCIAL
Dr. Rafael Gill Ramirez. Presidente Ejecutivo.
Avenida Pichincha con calle Guaicaipuro, Torre Alianza, piso 9.
Urb. El Rosal, Caracas
Tlf. 953.44.22/42.13..60.55/42.22/59.33/49.33/59.79
Fax: 953.75.78

BANGENTE
Sr. Juan Uslar Gathmann. Presidente Ejecutivo.
Avenida Bolívar cruce con Calle Washington N° 19., Catia.
Tlf: 873.20.03/ 873.21.42/8709.13.33/872.17.30
Fax. 870.08.64

SISTEMA NACIONAL DE AHORRO Y PRESTAMO (BANAP)
Dr. Oswaldo Ramirez Briceño. Presidente.
Av. Venezuela. Edif. BANAP, El Rosal, Caracas.
Tlf. 951.62.22. Fax. 951.71.27

DEL PUEBLO SOBERANO
Lic. Cándido Roberto Rodríguez. Presidente.
Av. Andrés Eloy Blanco de Gradillas a San Jacinto, Edif. Gallo de Oro. Caracas.
Tlf. 563.72.61/564.06.14. Fax. 564.33.01

INSTITUTOS MUNICIPALES

MUNICIPAL DE CREDITO POPULAR
Dr. Hender López B. Presidente (E):
Bloque 1 del Silencio, frente a la Plza O´Leary. Caracas.
Tlf: 481.75.30/481.66.07/482.83.15. Fax. 481.75.30

ENTIDADES DE AHORRO Y PRESTAMO

DEL SUR-ORIENTE, E.A.P
Dr. César Navarrete. Presidente.
3ra. Av. de Los Palos Grandes cruce con 1ra. Transv., Edif. Balmoral, P.B, detrás del Parque Cristal.
Tlf. 286.99.73./286.72.46. Tlf: (086)22.96.11/22.92.63/22.99.87
Fax: (086) 22.25.14

MERENAP
Dr. César Navarrete. Presidente.
Av. 4ta. entre Calle 24 y 25. Edif. Merenap, Merida, Estado Merida
Tlf. 074/404000. Fax. 074/526748

EMPRESAS DE ARRENDAMIENTO FINANCIERO

ARRENDAVEN
Dr. Nelson Mezerhane. Pesidente.
Centro Cremerca, Av. Venezuela, El Rosal. Caracas.
Tlf. 9513130/6022. Fax. 9515772

SOFITASA
Dr. Oscar Galeazzi Mogollón. Presidente.
Torre Sofitasa, 7ma. Av. c/c 10 San Critóbal, Edo. Táchira.
Tlf. (076) 446011/6526. Fax. (076) 446840/2370

UNION
Dr. Ignacio Salvatierra. Presidente.
Av. Universidad Esq. el Chorro piso 18. Caracas.
Tlf. 5018652/8654/7034. Fax. 5018666/8649

BANCOS HIPOTECARIOS

DE INVERSION TURISTICA DE VENEZUELA
Dr. Nelson Mezerhane. Presidente.
Centro Andrés Bello, Torre Este, piso 1 Avenida Andrés Bello, Caracas.
Tlf. 782.25.08 /781.25.11/782.91.24/782.81.19. Fax: 793-19-36

UNIDO, S.A.
Dr. Ignacio Salvatierra. Presidente.
Av. Este 2, N° 201, Edif. Banco Hipotecario Unido, Los Caobos. Caracas.
Tlf. 501.98.22/98.23. Fax. 501.98.29

VENEZOLANO, C.A.
Dr. Carlos Gill Ramirez. Presidente.
Edificio Torre del Desarrollo Av. Guaicaipuro entre Av. Principal de las Mercedes y Av. Pichincha, El Rosal
Tlf. 953.33.33 – 953.32.22. Fax. 953.02.23

BANESCO BANCO HIPOTECARIO
Sr. Fernando Crespo Suñer. Presidente.
Av. Principal de Las Mercedes, Edf. Banesco. Caracas.
Tlf. 952.70.74. Fax: 951.75.16

BANCOS DE INVERSION

BANPLUS, BANCO DE INVERSION
Sr. Remo Passariello P. Presidente.
Paseo Enrique Eraso. Entrada de San Román, Torre La Noria, piso 7. Las Mercedes. Caracas.
Tlf. 909.06.00/0603/06.47. Fax. 992.85.75
Doctora Febe Briceño de Haddad
Presidenta.

C.A. CAVENDES, BANCO DE INVERSION
Av. Francisco de Miranda Edif. Cavendes,
piso 17, Caracas.
Tlf. 285.82.75/283.85.57/26.22
Fax. 284.36.23
Doctor Julio Rodríguez, Presidente.

CENTRAL HIPOTECARIA BANCO DE INVERSION
Av. Libertador Edif. Libertador,
Multicentro Empresarial del Este,
Núcleo A piso 16, Chacao.
Caracas.
Tlf. 263.85.57/265.93.32/265.97.23/265.97.45 / Fax. 265.73.1

FEDERAL, BANCO DE INVERSION
Dr. Nelson Mezerhane. Presidente.
Centro Cremerca, Av. Venezuela Urb. El Rosal. Caracas.
Tlf. 901.50.11. Fax. 951.47.90/952.79.15

GALICIA DE VENEZUELA, BANCO DE INVERSIÓN
Dr. José Ramón Rodríguez Leiva. Presidente.
Av. Venezuela, Edif. Venezuela. Piso 1, Of. 11
Urb. El Rosal. Caracas.
Tlf: 952.30.93. Fax. 952.68.65

BANINVEST BANCO DE INVERSION, C.
Señor Carmelo De Stefano. Presidente.
Av. Páez (frente Plaza Madariaga).
Sede principal Universidad Santa María, piso 1, Urb. El Paraíso
Tlf: 481.09.92. Fax. 484.68.55

FIVCA
Dr. Fernando Alvarez Paz. Presidente
Av. México con calle Tito Salas, Edif. Santa María, piso 6. Caracas.
Tlf. 952.29.93/60.24/40.51/41.93. Fax. 952.62.82

UNION, BANCO DE INVERSION
Dr. Ignacio Salvatierra. Presidente.
Av. Universidad Esq. El Chorro, Torre Unión, piso 18. Caracas.
Tlf. 501.86.15/501.86.25/86.13/86.01. Fax. 501.86.49

ANEXO III

Ley sobre mensajes de datos y firmas electrónicas

HUGO CHÁVEZ FRIAS
PRESIDENTE DE LA REPÚBLICA BOLIVARIANA
DE VENEZUELA

En ejercicio de la atribución que le confiere el numeral 8 del artículo 236 de la Constitución de la República Bolivariana de Venezuela, en concordancia con el artículo 1, numeral 5, literal b de la Ley que autoriza al Presidente de la República para dictar Decretos con Fuerza de Ley en las Materias que se delegan, en Consejo de Ministros,

LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

CAPITULO I
AMBITO DE APLICACIÓN Y DEFINICIONES
Objeto y aplicabilidad del Decreto-Ley.

Artículo 1. El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en

un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas.

La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Definiciones.

Artículo 2. A los efectos del presente Decreto-Ley, se entenderá por:

Persona: Todo sujeto jurídicamente hábil, bien sea natural, jurídica, pública, privada, nacional o extranjera, susceptible de adquirir derechos y contraer obligaciones.

Mensajes de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Emisor: Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.

Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Signatario: Es la persona titular de una Firma Electrónica o Certificado Electrónico.

Destinatario: Persona a quien va dirigido el Mensaje de Datos.

Proveedor de Servicios de Certificación: Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley.

Acreditación: Es el título que otorga la Superintendencia de servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en este Decreto-Ley.

Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

Sistema de Información: Aquel utilizado para generar,

procesar o archivar de cualquier forma Mensajes de Datos.

Usuario: Toda persona que utilice un sistema de información.

Inhabilitación técnica: Es la incapacidad temporal o permanente del Proveedor de Servicios de Certificación que impida garantizar el cumplimiento de sus servicios, así como cumplir con los requisitos y condiciones establecidos en este Decreto-Ley para el ejercicio de sus actividades.

El reglamento del presente Decreto-Ley podrá adaptar las definiciones antes señaladas a los desarrollos tecnológicos que se produzcan en el futuro. Así mismo, podrá establecer otras definiciones que fueren necesarias para la eficaz aplicación de este Decreto-Ley.

Adaptabilidad del Decreto-Ley.

Artículo 3. El Estado adoptará las medidas que fueren necesarias para que los organismos públicos puedan desarrollar sus funciones, utilizando los mecanismos descritos en este Decreto-Ley.

CAPITULO II
DE LOS MENSAJES DE DATOS
Eficacia Probatoria.

Artículo 4. Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Sometimiento a la Constitución y a la ley.

Artículo 5. Los Mensajes de Datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal.

Cumplimiento de solemnidades y formalidades.

Artículo 6. Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica.

Integridad del Mensaje de Datos.

Artículo 7. Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Constancia por escrito del Mensaje de Datos.

Artículo 8. Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.

Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguiente condiciones:

1. Que la información que contengan pueda ser consultada posteriormente.

2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.

3. Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo.

CAPITULO III
DE LA EMISIÓN Y RECEPCIÓN DE LOS MENSAJES DE DATOS

Verificación de la emisión del Mensaje de Datos.

Artículo 9. Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensajes de Datos proviene del Emisor, cuando éste ha sido enviado por:

1. El propio Emisor.
2. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.
3. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente.

Oportunidad de la emisión.

Artículo 10. Salvo acuerdo en contrario entre las partes, el Mensaje de Datos se tendrá por emitido cuando el sistema de información del Emisor lo remita al Destinatario.

Reglas para la determinación de la recepción.

Artículo 11. Salvo acuerdo en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará conforme a las siguientes reglas:

1. Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.
2. Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de Datos en un sistema de información utilizado regularmente por el Destinatario.

Lugar de emisión y recepción

Artículo 12. Salvo prueba en contrario, el Mensaje de Datos se tendrá por emitido en el lugar donde el Emisor tenga su domicilio y por recibido en el lugar donde el Destinatario tenga el suyo.

Del acuse de recibo.

Artículo 13. El Emisor de un Mensaje de Datos podrá condicionar los efectos de dicho mensaje a la recepción de un acuse de recibo emitido por el Destinatario.

Las partes podrán determinar un plazo para la recepción del acuse de recibo. La no recepción de dicho acuse de recibo dentro del plazo convenido, dará lugar a que se tenga el Mensaje de Datos como no emitido.

Cuando las partes no establezcan un plazo para la recepción del acuse de recibo, el Mensaje de Datos se tendrá por no emitido si el Destinatario no envía su acuse de recibo en un plazo de veinticuatro (24) horas a partir de su emisión.

Cuando el Emisor reciba el acuse de recibo del Destinatario conforme a lo establecido en el presente artículo, el Mensaje de Datos surtirá todos sus efectos.

Mecanismos y métodos para el acuse de recibo.

Artículo 14. Las partes podrán acordar los mecanismos y métodos para el acuse de recibo de un Mensaje de Datos. Cuando las partes no hayan acordado que para el acuse de recibo se utilice un método determinado, se considerará que dicho requisito se ha cumplido cabalmente mediante:

1.Toda comunicación del Destinatario, automatizada o no, que señale la recepción del Mensaje de Datos.

2.Todo acto del Destinatario que resulte suficiente a los efectos de evidenciar al Emisor que ha recibido su Mensaje de Datos.

Oferta y aceptación en los contratos.

Artículo 15. En la formación de los contratos, las partes podrán acordar que la oferta y aceptación se realicen por medio de Mensajes de Datos.

CAPITULO IV
DE LAS FIRMAS ELECTRONICAS

Validez y eficacia de la Firma Electrónica. Requisitos.

Artículo 16. La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:

1.Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.

2.Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.

3.No alterar la integridad del Mensaje de Datos.

A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Efectos jurídicos. Sana crítica.

Artículo 17. La Firma Electrónica que no cumpla con los requisitos señalados en el artículo anterior no tendrá los efectos jurídicos que se le atribuyen en el presente Capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

La certificación.

Artículo 18. La Firma Electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16.

Obligaciones del signatario.

Artículo 19. El Signatario de la Firma Electrónica tendrá las siguientes obligaciones:

Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.

Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello.

El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

CAPITULO V
DE LA SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

Creación de la Superintendencia.

Artículo 20. Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Objeto de la Superintendencia.

Artículo 21. La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar, en los términos previstos en este Decreto-Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

Competencias de la Superintendencia.

Artículo 22. La Superintendencia de Servicios de Certificación Electrónica tendrá las siguientes competencias:

1. Otorgar la acreditación y la correspondiente renovación a los Proveedores de Servicios de Certificación una vez cumplidas las formalidades y requisitos de este Decreto-Ley, sus reglamentos y demás normas aplicables.
2. Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.
3. Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados.

4. Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.

5. Supervisar las actividades de los Proveedores de Servicios de Certificación conforme a este Decreto-Ley, sus reglamentos y las normas y procedimientos que establezca la Superintendencia en el cumplimiento de sus funciones.

6. Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.

7. Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.

8. Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.

9. Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.

10. Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.

11. Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.

12. Requerir de los Proveedores de Servicios de Certificación o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.

13. Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificados y sus usuarios, cuando ello sea solicitado por las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige esta materia.

14. Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.

15. Presentar un informe anual sobre su gestión al Ministerio de adscripción.

16. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.

17. Imponer las sanciones establecidas en este Decreto-Ley.

18. Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.

19. Las demás que establezcan la ley y los reglamentos.

Ingresos de la Superintendencia.

Artículo 23. Son ingresos de la Superintendencia de Servicios de Certificación Electrónica:

1. Los recursos que le sean asignados en la Ley de Presupuesto a través del Ministerio de Ciencia y Tecnología.

2. Los provenientes de su gestión conforme a lo establecido en esta Ley.

3. Cualquier otro ingreso permitido por ley.

De las tasas.

Artículo 24. La Superintendencia de Servicios de Certificación Electrónica cobrará las siguientes tasas:

1.Por la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de un mil unidades tributarias (1.000 U.T.).

2. Por la renovación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

3. Por la cancelación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

4. Por la autorización que se otorgue a los Proveedores de Servicios de Certificación debidamente acreditados con relación a la garantía de los Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros, conforme a lo establecido en el artículo 44 del presente Decreto-Ley, se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

Los Proveedores de Servicios de Certificación constituidos por entes públicos estarán exentos del pago de las tasas previstas en este artículo.

Mecanismos de control

Artículo 25. La Contraloría Interna del Ministerio de Ciencia

y Tecnología, ejercerá las funciones de control, vigilancia y fiscalización de los ingresos, gastos y bienes públicos sobre este servicio autónomo, de conformidad con la ley que regula la materia.

De la supervisión.

Artículo 26. La Superintendencia de Servicios de Certificación Electrónica supervisará a los Proveedores de Servicios de Certificación con el objeto de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz a sus usuarios. A tal efecto, podrá directamente o a través de expertos, realizar las inspecciones y auditorías que fueren necesarias para comprobar que los Proveedores de Servicios de Certificación cumplen con tales requerimientos.

Medidas para garantizar la confiabilidad.

Artículo 27. La Superintendencia de Servicios de Certificación Electrónica podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los Proveedores de Servicios de Certificación. A tal efecto, podrá ordenar, entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el Proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.

Designación del Superintendente.

Artículo 28. La Superintendencia de Servicios de Certificación Electrónica estará a cargo de un Superintendente, será de libre designación y remoción del Ministro de Ciencia y Tecnología.

Requisito para ser Superintendente.

Artículo 29. El Superintendente de Servicios de Certificación Electrónica, debe reunir los siguientes requisitos:

1. Ser venezolano.

2. De reconocida competencia técnica y profesional para el ejercicio de sus funciones.

No podrán ser Superintendente, los miembros directivos,

agentes, comisarios, administradores o accionistas de empresas o instituciones sometidas al control de la Superintendencia. Tampoco podrá ejercer tal cargo el que tenga parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad con personas naturales también sometidas al control de la Superintendencia.

Atribuciones del Superintendente.

Artículo 30. Son atribuciones del Superintendente:

1. Dirigir el Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.

2. Suscribir los actos y documentos relacionados con las materias especificadas en el artículo 22 de este Decreto-Ley.

3. Administrar los recursos e ingresos del Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.

4. Celebrar previa delegación del Ministro de Ciencia y Tecnología, convenios con organismos públicos o privados, nacionales e internacionales, derivados del cumplimiento de las atribuciones que corresponden a la Superintendencia de Servicios de Certificación Electrónica.

5. Elaborar el proyecto de presupuesto anual, de conformidad con las previsiones legales correspondientes.

6. Proponer escalas especiales de remuneración para el personal de la Superintendencia, de conformidad con las disposiciones legales aplicables.

7. Presentar al Ministro de Ciencia y Tecnología el Proyecto de Reglamento Interno.

8. Celebrar previa delegación del Ministro de Ciencia y Tecnología, los contratos de trabajo y de servicios de personal, que requiera la Superintendencia de Servicios de Certificación Electrónica para su funcionamiento.

9. Elaborar anualmente la memoria y cuenta de la Superintendencia de Servicios de Certificación Electrónica.

10. Las demás que le sean asignadas por el Ministro de Ciencia y Tecnología.

CAPITULO VI
DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Requisito para ser Proveedor.

Artículo 31. Podrán ser Proveedores de Servicios de Certificación, las personas, que cumplan y mantengan los siguientes requisitos:

1. La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

2. La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.

3. Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.

4. Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

5. Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación .

6. En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.

7. Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.

8. Las demás que señale el reglamento de este Decreto-Ley.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

De la acreditación.

Artículo 32. Los Proveedores de Servicios de Certificación presentarán ante la Superintendencia de Servicios de Certificación Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo 31. La Superintendencia de Servicios de Certificación Electrónica, previa verificación de tales documentos, procederá a recibir y procesar dicha solicitud y deberá pronunciarse sobre la acreditación del Proveedor de Servicios de Certificación, dentro de los veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud.

Una vez aprobada la solicitud del Proveedor de Servicios de Certificación, éste presentará, a los fines de su acreditación, garantías que cumplan con los siguientes requisitos:

1. Ser expedidas por una entidad aseguradora o bancaria autorizada para operar en el país, conforme a las disposiciones que rigen la materia.

2. Cubrir todos los perjuicios contractuales y extracontractuales de los signatarios y terceros de buena fe derivados de actuaciones dolosas, culposas u omisiones atribuibles a los administradores, representantes legales o empleados del Proveedor de Servicios de Certificación.

El Proveedor de Servicios de Certificación deberá mantener vigente la garantía aquí solicitada por el tiempo de vigencia de su acreditación. El incumplimiento de este requisito dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica.

Negativa de la acreditación.

Artículo 33. La Superintendencia de Servicios de Certificación Electrónica podrá negar la solicitud a que se refiere el artículo anterior, en caso que el solicitante no reuna los requisitos señalados en este Decreto-Ley y sus reglamentos.

Actividades de los Proveedores de Servicios de Certificación.

Artículo 34. Los Proveedores de Servicios de Certificación realizarán entre otras, las siguientes actividades:

1. Proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos.

2. Ofrecer o facilitar los servicios de creación de Firmas Electrónicas.

3. Ofrecer servicios de archivo cronológicos de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación.

4. Ofrecer los servicios de archivo y conservación de mensajes de datos.

5. Garantizar Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros.

6. Las demás que se establezcan en el presente Decreto-Ley o en sus reglamentos.

Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas Electrónicas que certifiquen, y la titularidad que sobre ellas tengan sus Signatarios.

Obligaciones de los Proveedores.

Artículo 35. Los Proveedores de Servicios de Certificación tendrán las siguientes obligaciones:

1. Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.

2. Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.

3. Verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico.

4. Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.

5. Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.

6. Informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su página en la Internet o

en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

7. Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.

8.Garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.

9.Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos.

10.Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su Inhabilitación Técnica.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la suspensión de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones establecidas en el presente Decreto-Ley.

La contraprestación del servicio.

Artículo 36. La contraprestación por los servicios que los Proveedores de Servicios de Certificación presten, estará sujeta a las reglas de la oferta y la demanda.

Notificación del cese de actividades.

Artículo 37. Cuando los Proveedores de Servicios de Certificación decidan cesar en sus actividades, lo notificarán a la Superintendencia de Servicios de Certificación Electrónica, al menos con treinta (30) días de anticipación a la fecha de cesación.

En el caso de Inhabilitación Técnica, el Proveedor de Servicios

de Certificación notificará inmediatamente a la Superintendencia de Servicios de Certificación Electrónica.

Recibida cualesquiera de las notificaciones señaladas en este artículo, la Superintendencia de Servicios de Certificación Electrónica emitirá un acto por el cual se declare públicamente la cesación de actividades del Proveedor de Servicios de Certificación como prestador de ese servicio, sin perjuicio de las investigaciones que pueda realizar a fin de determinar las causas que originaron el cese de las actividades del Proveedor, y las medidas que fueren necesarias adoptar con el objeto de salvaguardar los derechos de los usuarios. En ese acto la Superintendencia podrá ordenar al Proveedor que realice los trámites que considere necesarios para hacer del conocimiento público la cesación de esas actividades, y para garantizar la conservación de la información que fuere de interés para sus usuarios y el público en general.

En todo caso, el cese de las actividades de un Proveedor de Servicios de Certificación conllevará su retiro del registro llevado por la Superintendencia de Servicios de Certificación Electrónica.

CAPITULO VII
CERTIFICADOS ELECTRONICOS
Garantía de la autoría de la Firma Electrónica.

Artículo 38. El Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

Vigencia del Certificado Electrónico.

Artículo 39. El Proveedor de Servicios de Certificación y el Signatario, de mutuo acuerdo, determinarán la vigencia del Certificado Electrónico.

Cancelación.

Artículo 40. La cancelación de un Certificado Electrónico procederá cuando el Signatario así lo solicite a su Proveedor de Servicios de Certificación. Dicha cancelación no exime al Signatario de las obligaciones contraídas durante la vigencia del Certificado, conforme a lo previsto en este Decreto-Ley.

El Signatario estará obligado a solicitar la cancelación del Certificado Electrónico cuando tenga conocimiento del uso indebido de su Firma Electrónica. Si el Signatario en conocimiento de tal situación no solicita dicha cancelación, será responsable por los daños y perjuicios sufridos por terceros de buena fe como consecuencia del uso indebido de la Firma Electrónica certificada mediante el correspondiente Certificado Electrónico.

Suspensión temporal voluntaria.

Artículo 41. El Signatario podrá solicitar la suspensión temporal del Certificado Electrónico, en cuyo caso su Proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el Signatario.

Suspensión o revocatoria forzosa.

Artículo 42. En los contratos que celebren los Proveedores de Servicios de Certificación con sus usuarios, se deberán establecer como causales de suspensión o revocatoria del Certificado Electrónico de la Firma Electrónica, las siguientes:

1. Sea solicitado por una autoridad competente de conformidad con la ley.

2. Se compruebe que alguno de los datos del Certificado Electrónico proporcionado por el Proveedor de Servicios de Certificación es falso.

3. Se compruebe el incumplimiento de una obligación principal derivada del contrato celebrado entre el Proveedor de Servicios de Certificación y el Signatario.

4. Se produzca una Quiebra Técnica del sistema de seguridad del Proveedor de Servicios de Certificación que afecte la integridad

y confiabilidad del certificado contentivo de la Firma Electrónica.

Así mismo, se preverá en los referidos contratos que los Proveedores de Servicios de Certificación podrán dejar sin efecto la suspensión temporal del Certificado Electrónico de una Firma Electrónica al verificar que han cesado las causas que originaron dicha suspensión, en cuyo caso el Proveedor de Servicios de Certificación correspondiente estará en la obligación de habilitar de inmediato el Certificado Electrónico de que se trate.

La vigencia del Certificado Electrónico cesará cuando se produzca la extinción o incapacidad absoluta del Signatario.

Contenido de los Certificados Electrónicos.

Artículo 43. Los Certificados Electrónicos deberán contener la siguiente información:

1. Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.
2. El código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica.
3. Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.
4. Las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico.
5. La Firma Electrónica del Signatario.
6. Un serial único de identificación del Certificado Electrónico.
7. Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

Certificados electrónicos extranjeros.

Artículo 44. Los Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado

conforme a lo previsto en el presente Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado. Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

CAPITULO VIII
DE LAS SANCIONES
A los Proveedores de Servicios de Certificación

Artículo 45. Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando incumplan las obligaciones que les impone el artículo 35 del presente Decreto-Ley.

Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando dejen de cumplir con alguno de los requisitos establecidos en el artículo 31 del presente Decreto-Ley.

Las sanciones serán impuestas en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes o atenuantes existentes.

Circunstancias agravantes y atenuantes.

Artículo 46. Son circunstancias agravantes:

1. La reincidencia y la reiteración.
2. La gravedad del perjuicio causado al Usuario.
3. La gravedad de la infracción.
4. La resistencia o reticencia del infractor para esclarecer los hechos.

Son circunstancias atenuantes:

1. No haber tenido la intención de causar el hecho imputado de tanta gravedad.

2. Las que se evidencien de las pruebas aportadas por el infractor en su descargo.

En el proceso se apreciará el grado de la culpa para agravar o atenuar la pena.

Prescripción de las sanciones

Artículo 47. Las sanciones aplicadas prescriben por el transcurso de tres (3) años, contados a partir de la fecha de notificación al infractor.

Falta de acreditación.

Artículo 48. Serán sancionadas con multa de dos mil (2.000) a cinco mil (5.000) Unidades Tributarias (U.T.), las personas que presten los servicios de Proveedores de Servicios de Certificación previstos en este Decreto-Ley, sin la acreditación de la Superintendencia de Servicios de Certificación Electrónica, alegando tenerla.

Procedimiento ordinario.

Artículo 49. Para la imposición de las multas previstas en los artículos anteriores, la Superintendencia de Servicios de Certificación Electrónica aplicará el procedimiento administrativo ordinario previsto en la Ley Orgánica de Procedimientos Administrativos.

CAPITULO IX
DISPOSICIONES FINALES

Primera. El presente Decreto-Ley entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Segunda. Los procedimientos, trámites y recursos contra los actos emanados de la Superintendencia de Servicios de Certificación

Electrónica, se regirán por lo previsto en la Ley Orgánica de Procedimientos Administrativos.

Tercera. Sin limitación de otros que se constituyan, el Estado creará un Proveedor de Servicios de Certificación de carácter público, conforme a las normas del presente Decreto-Ley. El Presidente de la República determinará la forma y adscripción de este Proveedor de Servicios de Certificación.

Cuarta. La Administración Tributaria y Aduanera adoptará las medidas necesarias para ejercer sus funciones utilizando los mecanismos descritos en este Decreto-Ley, así como para que los contribuyentes puedan dar cumplimiento a sus obligaciones tributarias mediante dichos mecanismos.

Delitos informáticos,

delincuentes sin rostro

fue impreso por Fanarte

en el mes de septiembre de 2001.

Caracas, Venezuela

La **Fundación EnCambio** fue creada en mayo de 1996. Es una institución social que venido participando activamente en la búsqueda de salidas positivas a los problemas de nuestra sociedad. Unas de sus áreas fundamentales de trabajo es la prevención social integral.

Publicaciones

Revista Encambio
Venezuela tiene sed de justicia.
Diciembre de 1996.

La Descentralización:
La Inversión Rentable para el Futuro
Investigación de Argelia Rios
Coordinación de Carlos Tablante
Prólogo de Allan Brewer Carias
1997.

Una Verdadera Democracia
Texto: Ángela Zago
Ilustraciones: Félix Rodríguez
1998

Narcofinanciamiento Político
Una Visión Integral sobre Prevención y Control
Varios Autores
1998.

Suplemento sobre la Constituyente
Investigación: Pilar Suárez Sasso
1999

Poder Constituyente
Ricardo Combellas
Presentación: Hugo Chávez Frías
Prólogo: Carlos Tablante
1999-2000

Publicaciones "Cuentas Claras"
Editora: Margarita de Tablante
12 ediciones-2000-2001.

http:// www.preven.net/ encambio@telcel.net.ve.

«El ciberespacio es virtual, pero los delitos y abusos que ocurren en él son reales. Los daños, perjuicios, desilusiones y otras consecuencias que puede generar los hechos que representan los engaños producidos en la Internet pueden ser incuantificables y ruinosos para quienes sean defraudados...»

Fernando Fernández

«Considero un éxito el haber logrado el objetivo legislativo de culminar un anteproyecto de Ley sobre Delitos Informáticos. Con esta iniciativa se llena un vacio en nuestra legislación, y se responde a una necesidad formulada por la sociedad, quien se siente desamparada ante estos delitos de "segundo tipo"...»

Bayardo Ramírez Monagas

«Los vertiginosos cambios sociales ocasionados por el avance de la técnica, hacen de la reforma al Código Penal Venezolano, una imperiosa necesidad...»

Gregorio Quiñones Gómez

«La vulnerabilidad intrínseca que han demostrado los instrumentos digitales, y la falta de una regulación de carácter supranacional, produce un "terreno abonado" que favorece la comisión de muchas y muy variadas formas de fraudes y estafas a través de Internet...»

Jorge Luciani Gutiérrez

«Gracias a los resultados de la investigación desarrollada por la subcomisión parlamentaria dirigida por el diputado Tablante, se ha puesto de manifiesto la necesidad de un ordenamiento jurídico penal más amplio que una ley contra el fraude electrónico, de modo que su alcance permita proteger también otros bienes jurídicos...»

Beatriz Di Totto