El crimen en la Súper Red de Informática

Isabel C. Gandulla Díaz*

Introducción

La Súper Red de Informática, la Internet, la Infraestructura de Información Nacional, la Súper Autopista de Información Electrónica, la Red Mundial de Comunicación o simplemente la Red, son nombres diferentes para lo que es uno de los fenómenos tecnológicos más representativos de esta última década del siglo XX. Representa un mundo abierto a las posibilidades, los expertos estiman que para el 1998 habrá más de cien millones de usuarios de la Súper Red de Informática (en adelante Red), un número igual al de la población combinada de las seis ciudades más grandes del mundo.[1]

La Red es un sistema conectado de redes de comunicación.[2] Puede ser definida como un medio de comunicación de alcance mundial que transmite mensajes de manera simultánea desde un lugar remoto hacia otro. Actúa como un archivo mundial con información sobre miles de temas o muy bien como un centro de compras gigantesco. Este efecto se logra mediante una computadora personal y líneas de comunicación telefónica ordinarias. Dentro de la Red se incluyen los usuarios de correo electrónico, tablones de edictos electrónicos y grandes compañías como *América On Line*, *Compuserve* y *Prodigy*. El correo electrónico es un medio de comunicación mediante el cual la persona puede recibir o enviar mensajes o intercambiar información, todo en privado. Los tablones de edictos electrónicos, son lugares públicos en donde se pueden exponer o recibir mensajes. Por su parte las grandes compañías de computadoras proveen sus servicios para que los usuarios puedan conectarse por medio de la Red a otros sistemas.

---

*Estudiante de segundo año y miembro del Cuerpo de Investigadores, Redactores y Correctores de la *Revista de Derecho Puertorriqueño* de la Facultad de Derecho de la Pontificia Universidad Católica de Puerto Rico.

[1]Daniel Hu, Bill Lau and Kent Li, *Security in Cyberspace* (visitado el 28 de agosto de 1997) <http://logic.csc.cuhk.hk/~s951224/security.html>.

[2]Henry Edward, *The History of the Net* (visitado el 28 de agosto de 1997) <nethist8txtatumcc.umich.edu>.

La Red es una obra hecha por el hombre que representa la creación del primer organismo con inteligencia artificial capaz de crecer por sí mismo. Permite que dentro de esta vieja sociedad se cree una nueva, con un sistema de gobierno propio que ciertamente amenaza las libertades de algunos de sus usuarios. Hasta ahora la Red es como una sociedad joven que tiene sus propias formas de reglamentación, aunque estas son confusas. Esto se debe a que en el espacio cibernético, como se le llama a la zona donde todos los elementos mencionados en esta introducción habitan, las reglas cambian sumamente rápido.[3]

Es interesante saber que la visión original era que actuara como un medio para que exclusivamente científicos y profesores intercambiaran información. En la actualidad fluctúa con entre cuarenta y cincuenta millones de usuarios, siendo un campo abierto a personas de todas las edades y trasfondos socio-económicos.[4]

Este gran sistema de información comenzó en los años sesenta como un experimento militar de la Guerra Fría. Fue diseñada con el propósito de facilitar la comunicación militar y de los científicos en caso de que los Estados Unidos fueran devastados por un ataque nuclear de la Unión Soviética.[5] Contrasta su propósito original con su uso actual. En la Red se desarrolla un mundo abierto a las posibilidades, tanto para los ciudadanos respetuosos de la ley, como para los que no lo son. A través de este medio vemos como crece una sociedad nueva, que incuestionablemente desarrolla un sistema de gobierno propio, que pocos comprenden y que en ocasiones amenaza las libertades de algunos de sus usuarios. Según crecen los usos y el número de usuarios del espacio cibernético ha surgido un aumento en las actividades criminales relacionadas con las computadoras. Además es difícil asimilar los medios de reglamentación de este medio de comunicación, debido a la rapidez con que cambian.[6]

Es justo que el hecho del crecimiento de comportamientos con características criminales en la Red sea la preocupación mayor de esta autora. Este no es sólo un asunto sobre el futuro, sino que además trata sobre el presente. Es importante que se conozca la existencia del elemento criminal en la Red y cómo éste cobra auge. La comunidad debe ser informada sobre cuáles son los tipos de crímenes, qué tipo de

---

[3] *Id.*
[4] R. Otero, THE SECURITY ISSUES OF THE 90'S IN CORPORATE AMERICA 37 (1996).
[5] Edward, *supra* nota 3.
[6] Hu, Lau and Li, *supra* nota 2.

protección existe para los usuarios de la Red y si existe algún tipo de legislación diseñada especialmente para este asunto. Por otro lado los organismos pertinentes deben conocer alternativas viables para combatir estos actos que podrían catalogarse como delitos. Ante la actividad criminal y el inmesurable crecimiento de los usos de la Red es importante que se asegure algún grado de regulación. No sólo se trata de proteger a los usuarios de abusos o de ser expuestos a los ataques de estos criminales, se trata de proteger la inversión económica que estos han hecho en este complejo sistema de informática.

Esta es una oportunidad única de estudiar una nueva cultura desde su etapa de infancia para así asegurar la protección que necesitan los usuarios. Se ven indicios de que una libertad total infringe los derechos de otros. Una carencia total de regulación no asegura una justa participación a todos los usuarios. Hay que crear un método en el que los criminales ya existentes que se amparan en el anonimato que ofrece este medio e intensifican sus acciones delictivas, puedan ser llevados ante la justicia efectivamente.

I. Fuentes de Derecho

A. Estado actual de la ley respecto a la Red de Informática en Puerto Rico y en los Estados Unidos

Si se quiere mirar hacia el mañana se tiene que saber donde se está hoy respecto a los sistemas legales. Como el tema de la criminalidad por medio de la Red aún es novel, a continuación se examinará cuál ha sido la respuesta que la comunidad jurídica ha dado a estos tipos de crímenes de la Red, y si se ha hecho algún intento de legislación para prevenir posibles daños en la jurisdicción de Puerto Rico.

a. Discusión de leyes existentes en Puerto Rico

En Puerto Rico no se ha diseñado ningún conjunto de normas legales que regule a la Red y sus efectos. Sin embargo en el 1996 la legislatura puertorriqueña aprobó una legislación dirigida a las telecomunicaciones, la *Ley de telecomunicaciones de 1996.*[7] Esta ley expone que en Puerto

[7] Ley Núm. 213 de 12 de septiembre de 1996, art. I, 27 L.P.R.A. § 265.

Rico hay un interés por aumentar el uso de estos sistemas de comunicación electrónica y por proteger a las compañías que se dedican a facilitarlos. Esto se debe a que uno de los objetivos gubernamentales es que todos en Puerto Rico lleguen a tener acceso a estos medios de comunicación electrónica. Es por lo tanto que se le dará a las compañías la suficiente libertad para que ellas mismas velen por el desarrollo de estos medios dentro del país. El Estado buscará fomentar y preservar estos sistemas, pero lo hará sin intervenir directamente para regular. El legislador entiende que la regulación debe ser una consecuencia de las mismas fuerzas económicas, que funcione como una autoregulación. El gobierno no pondrá ninguna limitación innecesaria para que las compañías se puedan dedicar a su crecimiento.

Este primer artículo de la ley reitera que el gobierno no va a obstruir las operaciones de las compañías, sino que quiere ser un guardián del ambiente. Además deja claro que deben ser las mismas compañías las que busquen soluciones y solamente en última instancia es que se debe acudir a los foros judiciales. El compromiso es uno donde se velará por la libertad de acción asegurando que no se creen leyes limitantes a la capacidad de una compañía de telecomunicaciones.

La Ley[8] crea la Junta Reglamentadora de Telecomunicaciones de Puerto Rico (en adelante Junta) a la cual le otorga el poder para que decida y sea la primera en velar por cualquier procedimiento que se tenga que iniciar para que se cumpla lo propuesto por los legisladores. Por eso cuando el primer ciudadano puertorriqueño o compañía establecida en la isla sufra de un crimen cibernético será esta Junta la que determine los pasos a seguir para asegurar la protección y remedios adecuados a la situación particular que se presente. La Ley en sus artículos del uno al tres se dedica a definiciones relacionadas con este tema y en su parte (j) dispone:

> Compañía de telecomunicaciones, significará cualquier persona que posea, controle, administre, opere, maneje, supla o revenda, ya sea parcial o totalmente, directa o indirectamente, cualquier servicio de telecomunicaciones en Puerto Rico, incluyendo servicios de acceso a la **red**; disponiéndose que las compañías de cable que presten servicios de telecomunicaciones serán consideradas compañías de telecomunicaciones para propósito de este capítulo.[9]

---

[8]Ley Núm. 213 de 12 de septiembre de 1996, art. II-1, 27 L.P.R.A. § 267.

[9]Ley Núm. 213 de 12 de septiembre de 1996, arts. 1-3, 27 L.P.R.A. § 265a. (Énfasis

Es importante recalcar el que en esta definición se hace mención del término Red como uno dentro del mundo de las telecomunicaciones. Esta definición denota la intención del legislador de cubrir los medios de comunicación que le sea posible y a sus proveedores dentro de Puerto Rico. El texto de la ley confirma que los servicios tendrán todo el espacio que sea necesario para evolucionar y que la Junta será la encargada de que así sea, según se establezca de tiempo en tiempo y de acuerdo a las leyes federales relacionadas a las telecomunicaciones.

Por otro lado, el legislador define lo que son las telecomunicaciones diciendo: "a. Telecomunicaciones, significa la transmisión de información seleccionada por el usuario, entre puntos especificados por el usuario, sin que se cambie el formato o contenido de la información enviada y recibida."

La Red es un medio de telecomunicación que transmite información de un punto a otro, sin que se altere la comunicación o su contenido, por lo tanto es parte de la definición antes citada. La Junta tendrá jurisdicción en todos los asuntos de telecomunicaciones y sobre las personas que traten de perjudicar las actividades o intereses sobre los cuales la misma tiene poder. Ese poder de la Junta será sobre todo aquello que no esté en conflicto con las disposiciones federales de comunicación, así como aquellas normas federales que hayan ocupado el campo.[10] Es por lo tanto que este organismo actuará en todos aquellos espacios que quedan vacíos por razón de que las leyes federales no los han legislado. Este órgano regulador tiene poder y fuerza que le permite imponer multas de hasta veinticinco mil dólares de manera que se logre respeto y el desarrollo de un buen ambiente en el área de las telecomunicaciones.[11]

La ley antes discutida no fue hecha pensando en el crimen de las computadoras. Se explica este hecho porque en Puerto Rico hay sólo un puñado de casos que se refieren a computadoras. La mayoría las describen como herramientas de trabajo o bienes muebles, girando estos casos en torno a incumplimiento de contratos relacionados a programación de computadoras. Como se ha visto no ha habido

---

suplido.)
[10]Ley Núm. 213 de 12 de septiembre de 1996, art. II-6, 27 L.P.R.A. § 267 e.
[11]Ley Núm. 213 de 12 de septiembre de 1996, art. II-7, 27 L.P.R.A. § 267f.

controversia respecto a las computadoras como medios de telecomunicación. Esta ley no ha afectado a las compañías que dan el servicio de la Red en Puerto Rico, pero es sabido que ya ha provocado un gran impacto en la isla en el campo de las telecomunicaciones como han sido los servicios telefónicos y de celulares.

Sin duda la norma legal antes descrita es necesaria y es un intento por anticipar los cambios en el mundo de las telecomunicaciones. Aunque todavía no esté dirigida al crimen en las computadoras, ciertamente puede abrir la puerta a su examen. La Red como medio de telecomunicación quedaría sujeta a las regulaciones de esta ley y a la Junta. Deberá ser la Junta el organismo administrativo que vele por el justo desarrollo de la ley y podrá aplicar sus normas a un acto delictivo llevado a cabo en la Red.

b. Discusión de leyes existentes en los Estados Unidos

En los Estados Unidos la historia es diferente. Desde el 1978, cuarentinueve de los cincuenta Estados han hecho algún tipo de legislación relacionada con el crimen por computadora. Estos estatutos fueron creados durante el auge en el uso de computadoras personales que comenzó en los años setenta y velan por la seguridad de las transacciones que en aquel entonces eran capaces de hacer las mismas. Sobre la comunicación electrónica, no se tomaron en cuenta asuntos relacionados a seguridad o que serviría como un medio de comunicación instantáneo como lo es hoy. No fueron creadas para atender específicamente el crimen en el espacio cibernético, ya que éste toma auge en los últimos diez años.

El primer Estado en aprobar una ley de esta índole fue Florida en el 1978, luego le siguió Arizona, en ese mismo año.[12] A estas leyes estatales se le suman leyes federales que aplican a todos los Estados, inclusive a Puerto Rico. Algunas han sido diseñadas para atacar problemas específicos, como la *Ley de derechos de autor*.[13] Esta hace criminal la piratería de programas o información aún en el espacio cibernético. Entre las leyes federales más relevantes a la realización de este artículo se encuentran las que a continuación se describen.

---

[12]Otero, *supra* nota 5, pág. 32.
[13]17 U.S.C. § 506 (1995).

La *Ley para el Fraude y Abuso por Computadoras*[14] dispone que es una ofensa criminal el obtener bienes o propiedades de valor de manera fraudulenta mediante el uso de un equipo de comunicación. Estas acciones pueden ser castigadas como delitos graves con multas de miles de dólares y hasta veinte años de cárcel. La Ley *para Fraude y Actividades Relacionadas, en conexión con las Computadoras*[15] incluye a las computadoras entre los equipos o medios de comunicación que menciona la sección anterior.

La Ley del *Fraude por Medios de Comunicación por Cable*[16] establece que es una ofensa federal el defraudar para obtener dinero o bienes por medio de radio, televisión o comunicación por cable. Es interesante que esta Ley estima que bastará con lograr preponderancia de la prueba para procesar a los infractores, una vez se pruebe que la Red cuenta como una de las formas de comunicación por cable que el estatuto describe.

La Ley *Racketeer Influenced and Corrupt Organization* (R.I.C.O.)[17] podría ser aplicada exitosamente para procesar casos de fraude por computadoras y telecomunicaciones si satisfacen los elementos necesarios para su aplicación, haciendo una queja de que una persona participó para defraudar y obtener ilegalmente el acceso secreto de la víctima a un sistema de computadoras y así obtener información en por lo menos dos actuaciones dentro de un periodo de diez años. Un estatuto semejante al R.I.C.O. es el que trata sobre *transportación de bienes robados, seguros, dinero, sellos de impuestos estatales fraudulentos o artículos usados para falsificación.*[18] Este considera un fraude el tomar bienes mercancía o cualquier otra información robada que sea transferida por computadoras u otras líneas de comunicación de una computadora a otra por los medios de comunicación estatales.

Son muchas las leyes que se pueden adaptar a las situaciones del crimen por computadoras. Aunque los Estados han aprobado leyes dedicadas al crimen por computadoras, aún son escasas las que se han hecho específicamente para el crimen en el espacio cibernético. Por eso en ocasiones al tratar de adaptar leyes al criminal de la Red los jueces se

[14] 18 U.S.C. § 1029 (1986).
[15] 18 U.S.C. § 1030 (1984).
[16] 18 U.S.C. § 1334 (1985).
[17] 18 U.S.C. § 1961 (1970).
[18] 18 U.S.C. § 2314 (1948).

ven en la difícil situación de dejarlos libres de amonestación. Es penoso el que como no se dieron los elementos de los delitos ya clasificados y sabiendo que se ha hecho algo malo, no se pueda castigar a los criminales del espacio cibernético.

La Red nos ha facilitado la vida en muchos aspectos pero nos la complica y complicará en otros tantos. En el caso *Reno, Attorney General v. American Civil Liberties Union*[19] varias provisiones de la *Ley para Decencia en la Comunicación de 1996*[20] que buscaban proteger a menores de material obsceno en la Red fueron atacadas constitucionalmente. La ley[21] específicamente hace criminal la transmisión de mensajes obscenos o indecentes a menores de dieciocho años de edad, prohibiendo su envío. Además se exige a las compañías o personas que ofrecen estos servicios de orientación sexual o violenta, que traten de restringirle el paso a los menores pidiéndole a los interesados en accesarlos números de tarjetas de crédito o número de identificación para asegurarse de que sean adultos.

Al ser revisada se encontró que estas provisiones atacan la libertad de expresión protegida por la Primera Enmienda de la Constitución de los Estados Unidos. Los ataques constitucionales a la *Ley para Decencia en la Comunicación de 1996*[22] cuestionaban cuán efectivo sería el estatuto para cumplir con su meta de proteger a los menores de la exposición a material indecente en la Red. La mayor dificultad fue que la Red es de alcance mundial, mientras el estatuto queda limitado a los Estados Unidos.[23]

La médula de este asunto es que existen criminales y crímenes en la Red y los usuarios necesitan protección contra ellos, prácticamente existe un vacío legal en esta materia. Tanto en Puerto Rico como en los Estados Unidos, ni las leyes, códigos o reglas han sido creados para enfrentar específicamente este tipo de crimen. Por otro lado los escasos intentos de legislación que se han hecho, según expuestos anteriormente, no han logrado un método que se le pueda imponer a la variedad multinacional de usuarios que hay en este medio de comunicación. Existe una seria complicación cuando se trata de establecer qué jurisdicción atenderá en

---

[19]117 S. Ct. 2329 (1997).
[20]47 U.S.C. § 223, *et seq*.
[21]47 U.S.C. § 223(a)(1)(B)(ii)(Supl. 1997).
[23]23 47 U.S.C. § 223, *et seq*.
[23]Nesson Marglin, *The Day the Internet Met the First Amendment: Time and the Communications Decency Act*, 10 HARV. J. I. & TECH. 113 (otoño 1996).

un caso cuando las víctimas y los criminales pueden estar en distintas partes del mundo.

II. Surge el crimen en el espacio cibernético

Continuando con este tema se expondrá como es que llega el elemento criminal a este medio de información. En la actualidad, prácticamente cualquier persona está consciente de la existencia de la Red y de su rápido crecimiento. Este increíble crecimiento ha traído consigo la aparición del elemento criminal. No obstante este aumento no ha traído realmente nuevos tipos de crímenes o de criminales, sino que le ha dado un nuevo ambiente en el cual los crímenes o criminales de siempre puedan incrementar sus actividades.[24] En esencia la Red le ha dado a los viejos criminales nuevas herramientas para expresar un comportamiento criminal tradicional.[25] Para entender mejor esta nueva zona de crimen se examinará al criminal del espacio cibernético.

A. Quiénes son los *hackers* y *crackers* de la Red

El diccionario de los *hackers* los define así: "Una persona que disfruta de explorar los detalles de sistemas de programación para expandir sus capacidades y conocimientos, contrario a la mayoría de los usuarios quienes prefieren aprender sólo el mínimo necesario."[26]

Los *hackers* son los criminales del espacio cibernético, andan tratando de entrar a áreas prohibidas, mientras que un *cracker* es una especie más agresiva de *hacker*. El *cracker* anda con intenciones malignas en lugar de una mera curiosidad. La mayoría de los *hackers*, que no son destructivos son producto de la generación de computadoras. Estos están entre las edades de dieciséis y veinticinco años y el noventa y nueve punto nueve por ciento son inofensivos. Están muy bien organizados y se reúnen en una convención anual para compartir sus estrategias sobre cómo entrar a sistemas, aparentemente, seguros.[27] El intruso de computadoras y sistemas

---

[24]Daniel M. Rosen, *Hackers and Crackers: the Myth Debunked* (visitado el 28 de agosto de 1997) <http://actlab.utexas.edu/~aviva/compsee/ cracker.html>.
[25]Otero, *supra* nota 5, pág. 58.
[26]*Id.* pág. 26.
[27]*Id.* pág. 58.

de computación disfruta de dos factores; que su crimen es prácticamente invisible y que hay un bajo grado de detenciones.

Contrario a lo que el público piensa de ellos, los *hackers* no son expertos en computadoras que están todo el tiempo en su casa. Muchos son jóvenes adultos con expedientes criminales en crímenes relacionados a computadoras que cometieron desde sus propias casas siendo aún menores de edad. El *hacker* piensa que todos los programas y la información en el espacio cibernético deben ser de dominio público. Entran en los sistemas buscando conocimiento sobre nuevas computadoras, sistemas de seguridad y claves de acceso. Los retos más grandes son sistemas que contengan secretos, como los del Departamento de Defensa y compañías de comunicación o de computadoras. Cuando tienen éxito publican la información en tablones de edictos electrónicos en la Red, en sus propias revistas, programas de radio o en sus convenciones anuales, donde comparten la información e ideas de cómo entrar a otros sistemas.[28]

Algunos piensan que estos criminales se perfeccionaron por necesidad. Durante la Guerra Fría, los controles occidentales le privaron a muchos científicos en instituciones militares de Rusia y países del Este Europeo de la información tecnológica más reciente. Siendo así, tenían que mantener el paso de sus enemigos de alguna manera. El resultado es que la mayoría de los programadores más creativos y a la misma vez los *hackers* potencialmente más peligrosos viven y trabajan en partes del mundo que aún tienen inestabilidad política y problemas económicos.[29]

Cinco jóvenes que son *hackers*, residentes en Nueva York, apodados *Masters of Disaster* (maestros del desastre) fueron arrestados y sentenciados por lograr acceso ilegal al Departamento de Defensa, a compañías financieras y de telecomunicaciones mediante sus sistemas de computadoras conectados por toda la nación Norteamericana. Se les arrestó por vender información, inclusive reportes de estados de crédito.[30]

Al criminal de la Red le gusta el reto que representa el entrar dentro de un sistema y el conocer secretos que nadie más puede saber. En ocasiones se conforman con entrar y observar lo que hay en ese lugar, en otras alteran lo que encuentran en ese espacio y en otras inclusive se

---

[28] *Id.* pág. 26.
[29] Cooper, *Infowar Con: Conference Wrap-up*, CORPORATE SECURITY 5 (10 de marzo de 1995).
[30] Kluepfel, *A Recipe for Hacker Heartburn*, SECURITY MANAGEMENT 40 (enero 1995).

apoderan de la propiedad o la destruyen. Típicamente son jóvenes interesados en las computadoras que se entusiasman por este campo, aprenden rápido y consiguen trabajo en compañías relacionadas con computadoras, lo que les permite estar dentro del negocio y así poder hacer sus andanzas. Por eso es que los empleados descontentos son el grupo más común de *hackers*. Los empleados de grandes compañías frecuentemente accesan información más allá de sus niveles de seguridad o se aprovechan de sus claves de acceso para extorsionar o sobornar a sus jefes.[31] El fraude por computadora conocido como *hacked* le da al intruso el acceso a las computadoras de negocios con el propósito de:

a. Maliciosamente destruir, cambiar o copiar archivos, programas o sistemas.

b. Invadir la privacidad para obtener información ya sea para venderla o por pura diversión.

c. Borrar sus huellas; entrando al sistema de una compañía y luego a otro para que no puedan encontrar al intruso original.[32]

En una reciente encuesta, más del setenta por ciento de las compañías relacionadas con computadoras fueron atacadas por la actividad de los *hackers* en los pasados cinco años.[33]

Los creadores de programas son otro grupo que comúnmente entra a sistemas de computadoras para supuestamente ver si los sistemas de seguridad de la compañía son efectivos o no.[34] Por eso mismo es que muchas compañías y el gobierno están contratando *hackers* como jefes de sus equipos de seguridad.[35] El otro tipo de *hacker* es el que se dedica a hacer maldades. Típicamente es un joven adolescente que entra a otros sistemas de computadoras para satisfacer su curiosidad por saber qué es lo que contienen otros sistemas.[36]

Entre junio y octubre de 1994, el ruso Vladimir Levin, un *hacker* de computadoras y jefe de un sistema operativo en una compañía de programación en Rusia, descubrió y entró al sistema de transferencias de

---

[31]Ian Davis, *Crime and the Net: an Overview of Criminal Activity on the Internet and the Legal Community's Response* (visitado el 28 de agosto de 1997) <http://www.cybersquirrel.com/clc/index.html>.
[32]Otero, *supra* nota 5, pág. 24.
[33]Cunningham, *The Hall Crest Report II: Private Security Trends 1970-2000,* MCLEAN VIRGINIA: HALL CREST SYSTEMS, INC., 20 (1990).
[34]*Id.*
[35]Kluepfel, *supra* nota 31.
[36]Davis, *supra* nota 32.

fondos bancarios electrónico del *Citibank*. Levin movilizó más de diez millones de dólares a cuentas en Finlandia, Rusia, Alemania, Estados Unidos e Israel, entre otros. Las transacciones se hicieron mediante el sistema de transferencia de fondos bancarios en el departamento de *Wall Street* del *Citibank*. Aunque el sistema de seguridad del banco percibió algunas claves de las transacciones fraudulentas Levin fue exitoso hasta que finalmente fue arrestado en Londres. Se está procesando su extradición hacia los Estados Unidos. La mayor parte de los fondos robados fueron recuperados exitosamente.[37]

Esta situación legal produce la exposición que a continuación presenta uno a uno los tipos de crímenes que la autora ha logrado identificar en el espacio cibernético, en qué consisten y qué se puede hacer respecto a éstos. Cada uno de los crímenes serán acompañados de casos verídicos que demuestran el alcance de estas fechorías. Como parte de esta exposición se desarrollará una comparación de algunos de los crímenes identificados en el espacio cibernético y algunos de los delitos tipificados en el Código Penal de Puerto Rico. Luego de esta comparación se estará en posición de hacer un análisis para llegar a la conclusión de que algunos de los actos llevados a cabo por los usuarios de las computadoras podrían tipificarse como delitos en el ordenamiento jurídico puertorriqueño. Esto al amparo del Código Penal de Puerto Rico.

III. Exposición

A. Un diccionario para el crimen cibernético

1. Apropiación de claves secretas

La apropiación de claves secretas se logra mediante unos programas de computadoras capaces de monitorear y grabar el nombre de un usuario y su clave secreta de acceso a un sistema. Se hace en el momento que están tratando de accesar y como resultado queda en riesgo la seguridad y la privacidad de ese sistema y del usuario.[38] Se trata de tomar para sí una clave electrónica que no es la propia y utilizarla fraudulentamente con la

---

[37] *Citibank Hit Fraud Attacks on Two Fronts,* CORPORATE SECURITY 4 (25 de agosto de 1995).

[38] Natalie D. Voss, *Jones Telecommunications and Multimedia Encyclopedia: Crime on the Internet* (visitado el 13 de noviembre de 1996) <http://www.digitalcentury.com/encyclo/update/>.

intención de accesar para ver, dañar o apropiarse de propiedad electrónica. Como hoy en día la tendencia es que cada vez más universidades, compañías y agencias se conectan a la Red, vemos un número mayor de información que queda expuesta a ser literalmente vista y usada por cualquiera que tenga esta tecnología.

El programa dedicado a la apropiación de claves secretas monitorea la actividad de las máquinas conectadas al sistema, para poder identificar los nombres de los usuarios y sus claves secretas. Una vez tienen estos datos se puede personificar al usuario autorizado dándole al criminal un acceso directo a cualquier documento o archivo.[39]

2. Bombas a direcciones electrónicas

Una vez el usuario tenga su dirección electrónica podrá recibir correo electrónico. En un correo electrónico ese usuario es capaz de acumular docenas de mensajes, leer los que le interesen primero, guardar los menos importantes para después. Además se guardan las direcciones de las personas a quienes se quiere accesar.

Cuando llega una bomba disfrazada como un mensaje amistoso, y en realidad es un programa bomba, lo que ocurre es una explosión dentro del correo. Una vez se abre la bomba ésta estalla llenando el correo de miles de mensajes que lo sobrecargan y terminan sacando al usuario del sistema o llenando su correo de mensajes que deben ser sacados uno a uno.[40] El resultado craso de esa bomba es que se destruye toda la información electrónica que se tiene archivada en el correo, dejando al usuario con un correo electrónico inservible.

3. Drogas

Sorprendentemente hay drogas en el espacio cibernético. Recientemente la Policía de Puerto Rico quedó alertada y en vías de una investigación ya que se le informó sobre varios tipos de drogas que están cobrando auge en la isla. Las drogas se usan entre los asistentes a clubes y discotecas del país. Entre las más usadas está la "píldora del amor" o

---

[39]Deborah Russell and Elizabeth D. Zwicky, How to Get a Handle on Internet Security (visitado el 1 de octubre de 1997) <http://www.ora.com/oracom/issue5/inetsec.html>.

[40]Rothbar, *Rothbar's Revenge & Retribution Site* (visitado 24 de agosto de 1997) <htpp://pages.prodigy.com/rothbert/index.html>.

"éxtasis" que aumenta el apetito sexual del usuario. Este auge se estima que responde a la escasez de drogas como la cocaína y la heroína.

Gracias a la Red los jóvenes obtienen las recetas con cantidades y procedimientos a seguir para preparar las drogas ilegales. Aunque la policía local sabe muy poco sobre este asunto se prepara una investigación al respecto ya que se relaciona esta práctica por medio de las computadoras con una violación perpetrada a una joven después de que ésta quedara bajo efectos de una de estas drogas.[41]

Así vemos que llegan a Puerto Rico los efectos negativos de la libertad que se disfruta en la Red. La autora de este artículo en una de sus primeras experiencias en un cuarto de charlas para adolescentes mejor conocido como *chat room* pudo percatarse de como varios de los jóvenes hablaban libremente y de manera pública sobre drogas. Luego de varias discusiones y preguntas acordaron un precio para el producto ilegal, entonces uno de ellos invitó a los interesados a un "cuarto privado" donde se les informaría cómo contactar un agente vendedor en su ciudad. Una vez se pasa a un "cuarto privado" se bloquea la comunicación abierta y solo pueden participar los que tengan acceso a esa zona por lo cual se pierde el contacto.

Existe un cuarto en la Red donde hay ciento setentinueve recetas de drogas. Informa cuál es el nombre común y el científico, cuáles son los componentes químicos, el procedimiento para prepararlas, dice cuál es la dosis recomendada e inclusive narra los efectos inmediatos, secundarios y a largo plazo de su uso.[42] Además se consiguen varias conexiones, especialmente alemanas, con recetas, técnicas de uso de drogas, fotos violentas y hasta se pueden conseguir virus para computadoras que pueden ser grabados o enviados a cualquier sistema. En otro cuarto se puede encontrar una receta para hacer *lysergic acid diethylamide* (L.S.D.) casero. Adjunto a la receta se encontraban comentarios de personas que ya la habían preparado y tratado. Algunos escribían para dar las gracias, otros para hacer comentarios, fueran positivos o negativos. Figuraban entre los que estaban allí comentando, jóvenes en Los Angeles, California y hasta una mujer de Moscú, Rusia que pedía una alternativa a un ingrediente que no podía conseguir en su país.

---

[41] Wapa Televisión, NOTICENTRO CUATRO, 22 de septiembre de 1997.

[42] Alexander Shulgin, *Pihkal a Chemical Love Story* (visitado 24 de septiembre de 1997) <http://www.hyperreal.org/drugs/pihkal>.

4. Escalamientos en la Red

Se le llama escalamiento a las ocasiones en que una persona penetra en la propiedad de otra con la intención de apoderarse de algo. Los escalamientos en la Red típicamente se logran usando herramientas de programación instaladas en una computadora en un lugar remoto. Una vez logran accesar pueden robar información, inyectar virus o causar problemas al cambiar los nombres de usuarios o sus claves secretas.[43] Se escala y penetra a la propiedad del usuario de la Red por medio del espacio cibernético con la intención de apoderarse o dañar los bienes electrónicos allí guardados. Este crimen es tan sofisticado y tan difícil de prevenir que algunos expertos estiman que entre un ochenticinco y un noventisiete por ciento de los escalamientos nunca son detectados.[44]

Es interesante que según más y más compañías buscan los beneficios de estar conectados a la Red, cada vez habrá más información que se pueda encontrar y podrá ser robada. Lamentablemente la mayoría de los escalamientos en la Red no se reportan, porque las compañías no quieren que los competidores sepan que sus sistemas son vulnerables.[45] El atractivo que hay en estos crímenes es que el crimen por computadora puede dejar más ganancias que otros tipos de fraude, por eso atrae a criminales en busca de grandes sumas de dinero. En el otro extremo los crímenes por computadoras muchas veces se cometen para lograr un reto, sin ninguna intención económica.[46]

A continuación un caso en el que se pudo detectar el escalamiento porque el fin del mismo era que fuese notado. El sábado 17 de agosto de 1996 unos *hackers* escalaron la página central del Departamento de Justicia de los Estados Unidos. Alteraron la página con suásticas y fotos obscenas. Había fuertes críticas a la *Ley para Decencia en la Comunicación de 1996*,[47] la próxima página estaba cubierta por suásticas

---

[43]Voss, *supra* nota 39.
[44]Michael J. Norton, *Review of Legal Resources: Computer Crime: a Crime Fighter's Handbook*, 25 FEB. COLO. LAW 49 (1996).
[45]Clinton Wilder, *How Safe is the Internet?* (visitado el 28 de agosto de 1997) <http://techweb/iw/509/05iuge.htm> (citando a Mark Rasch un abogado de Washington que ha procesado a varios *hackers*).
[46]Dave Icove, Karl Seger & William Von Storch, *Fighting Computer Crime* (visitado el 13 de noviembre de 1996) <http://www.ora.com?oracom/crime/crime1.html>.
[47]47 U.S.C. § 223, *et seq*.

color gris y en el tope leía: "Esta página es en violación a la ley para decencia en la comunicación." Debajo aparecía una foto a colores de Adolfo Hitler a quien compararon con Janet Reno la procuradora general de Estados Unidos.[48]

En el caso de *Steve Jackson Gómez v. U.S.*,[49] se debate si el usar una computadora para entrar a un tablón de edictos electrónico, que a su vez contenía correo electrónico privado archivado allí esperando a ser leído, constituye una entrada ilegal bajo el *Federal Wiretap Act*[50] según enmendada por el título I de la *Ley para la Privacidad en las Comunicaciones Electrónicas de 1986.*[51] En el caso se estaba tratando de procesar criminalmente a un invasor y encontraron que la ley actual no contempla nada sobre las telecomunicaciones, únicamente observaba las comunicaciones por cable *(wire).*

5. Espionaje

Cuando una persona entra a un lugar indebido con el propósito de saber qué está ocurriendo allí, e informárselo a otras personas, se está cometiendo espionaje. En el mundo de la tecnología los espías son considerados por algunos como herramientas de trabajo, para otros son un dolor de cabeza. Tanto las compañías como individuos y el gobierno adoran la oportunidad de espiar y ver qué están haciendo sus enemigos. La Red les está facilitando el acceso a información que antes era totalmente inaccesible.[52]

El entrar y salir, prácticamente, a diario de las computadoras del gobierno de los Estados Unidos es algo común y corriente.[53] El problema principal es que las compañías que son sujetos de ataques de espionaje son las mismas que lo practican con sus competidores. El espionaje electrónico industrial y el sabotaje son técnicas comúnmente usadas por los creadores de programas para asegurarse que su producto disfrutará de una superioridad en el ambiente técnico.[54] El problema se agrava ya que

---

[48]Associate Press, *Hackers Deface Web Site of U.S. Justice Department*, LOS ANGELES TIMES, 18 de agosto de 1996, pág. 20a (traducción nuestra).
[49] 36 F. 3d 457 (1994).
[50]18 U.S.C. § 2510, *et seq*. (1968).
[51]Pub. L. No. 99-508 Title I, 100 Stat. 1848 (1986).
[52]Voss, *supra* nota 39.
[53]Davis, *supra* nota 32.
[54]Otero, *supra* nota 5, pág. 58.

las mismas compañías contratan *hackers* profesionales para que les traigan información de otras compañías sobre el desarrollo de nuevos productos y estrategias de mercadeo.[55]

Kevin Poulsen fue el primer *hacker* que fue procesado por espionaje computadorizado. Fue tan exitoso al entrar a sistemas, tanto de gobierno como militares, que se le ofreció un puesto con la industria de defensa como un asesor de seguridad del sistema del Pentágono de los Estados Unidos. Al final regresó a sus malos pasos, conspiró para robar órdenes militares clasificadas, entró y arruinó una investigación del *Federal Bureau of Investigation* (F.B.I.). Finalmente fue acusado de espionaje y posesión de documentos clasificados, sorprendentemente en lugar de desistir entró a la computadora del F.B.I. y trató de sabotear su propia investigación, destruyendo la evidencia de todos sus crímenes. Actualmente está esperando juicio.[56] Este caso es una clara muestra de que esta práctica de fomentar el espionaje termina dando la vuelta y atacando a quien lo protegía.

6. Fraude en las tarjetas de crédito

En el 1995, doscientos sesentidos y medio millones de dólares de los trescientos cincuenta millones proyectados a hacerse en negocios, se hicieron en la Red, con dos y medio millones de usuarios comprando "en línea".[57] Casi todos estamos convencidos de que en el futuro miles de transacciones comerciales se harán mediante la Red, pero la herramienta más importante para lograr acceso a este comercio no será su computadora personal, será su tarjeta de crédito.

La preocupación es que es posible que capten sus dígitos económicos una vez usted los exponga en la Red.[58] La amenaza existe; por ejemplo, la página de la Red *Credit Wiz* contiene un programa de crimen de tarjetas de crédito, llamado *AOHell*, el cual sigue circulando y es un gran peligro para la industria. Este programa tiene la capacidad de generar y arreglar tarjetas de crédito y sus números, además crea nombres ficticios, direcciones y números de teléfono. Añade el nombre de una ciudad y

---

[55] Voss, *supra* nota 39.
[56] FREEDOM MAGAZINE, *A Crime By Any Other Name* (visitado el 28 de agosto de 1997) <http://www.thetha.com/goodman/crime.htm>.
[57] Finke, *On Line Cops and Robbers,* VIRTUAL CITY 9 (1996).
[58] *Credit Card Concerns* (visitado el 24 de agosto de 1997) <http://hest.net/credit.html>.

código de área contribuyendo a que parezca más real. El sistema funciona con *América On-Line* y corre con la versión de *Windows*. Con este sistema se pueden hacer cuentas falsas y permite que se obtenga información de los usuarios, como sus números de tarjeta de crédito y sus claves secretas.[59] Una vez se apoderan de esta información pueden hacer transacciones fraudulentas que serán cubiertas por el crédito de la víctima.

7. Hostigamiento

Muchas personas, especialmente mujeres, están siendo víctimas de hostigamiento en la Red.[60] El hostigamiento llega de personas que se han conocido mediante la misma Red y las herramientas son, los cuartos de conversación *chat rooms*, su correo electrónico o mensajes expuestos en tablones de edictos electrónicos.[61] Las víctimas de este crimen no reciben la protección adecuada por la falta de leyes para ser utilizadas contra este tipo de comportamiento.[62]

En el caso *U.S. v. Jake Baker*,[63] se presenta un intento para procesar criminalmente a Jake Baker. Bajo la *Ley para comunicaciones interestatales*[64] se le acusó de transmitir amenazas de lastimar o secuestrar a otra persona, mediante mensajes de correo electrónico. Todos los mensajes expresaban o un interés sexual o violencia contra las mujeres y niñas. La identidad estaba celosamente protegida, lo que sí se sabía era que se usaba una computadora localizada en Canadá y que a él le gustaba enviar mensajes que denominaba "sexo real".

La ley[65] que se pretendía usar para procesar a Baker establece: "Whoever transmits in interstate or foreign comerce any communication containing any threat to injure the person or another, shall be fined under this title or imprisioned not more than five years, or both."

---

[59]William, *Into the Future: a Look at the 21st Century,* LAW ENFORCEMENT TECHNOLOGY 15 (septiembre-octubre 1987).
[60]Wayne T. Price, *Harrasment Goes On Line: Low Tech Problem Hits Pc Networks,* U.S.A. TODAY, 1b (6 de agosto de 1996).
[61]*Id.*
[62]Gene Barton, *Taking a Byte Out of Crime: E-Mail Harrasment and the Inefficancy of Existing Law,* 70 WASH. L. REV. 465 (1995).
[63]104 F.3d 1492 (1997).
[64]18 U.S.C. § 875(c) (1948).
[65]*Id.*

Claro está hay que saber diferenciar entre lo que es una amenaza y lo que son expresiones protegidas por la Primera Enmienda de la Constitución de Estados Unidos. Tristemente en este caso se decide a favor del criminal. A continuación el razonamiento del Tribunal:

> Baker is being prosecuted under 18 U.S.C. 875(c) for is use of words, implicating fundamental First Amendment concerns. Baker's words were transmitted via means of the Internet, a relatively new communications medium that is itself currently the subject of much media attention. The Internet makes it possible with unprecedented ease to achieve world-wide distribution of material, like Baker's story, posted to its public areas. When used in such a fashion, the Internet may be likened to a newspaper with unlimited distribution and no locatable printing press--and with no supervising editorial control. But Baker's e-mail messages, on wich the superseding indictment is based, were not publicly published but privately sent. While new technology such as the Internet may complicate analysis and may sometimes require new or modified laws, it does not in this instance qualitatively change the analysis under the statute or under the First Amendment. Whatever Baker's faults, and he is to be faulted, he did not violate 18 U.S.C. 875(c).

Como Baker no usó tablones de edictos electrónicos que son públicos y por el contrario usó el correo electrónico que es privado, aunque hostigó, amenazó y realmente fue causante de esa conducta negativa, no violó la ley.

Se estima que hay aproximadamente doscientos mil hostigadores en los Estados Unidos.[66] El hecho de que en la Red prácticamente no existe regulación le asegura a estos hostigadores un nivel de inmunidad sobre su actuación culposa.[67] Además podría ser que este anonimato contribuya a que personas quienes normalmente no se comportarían de esa manera se animen a hostigar a otros usuarios.

El caso de hostigamiento por computadoras que despertó el interés de la autora en la actividad criminal en la Red fue el que a continuación presenta. Un hombre de Fresno, California, era el sospechoso de ser un hostigador por computadoras de alcance internacional. Se le ordenó no usar la Red hasta el día de su juicio en donde se ventilarían ciento doce cargos de fraude por computadoras. La fianza para Mark E. Johnson, de cuarenta años, fue de diez mil dólares. Se le ordenó a "Vito", su

---

[66]Robert A. Guy Jr., *The Nature and Consitutionality of Stalking Laws,* 46 VAND. L. REV. 991-995 (1993).

[67]Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace,* 104 YALE L. J. 1639, 1642 (1995).

seudónimo en computadora, que no molestara a las docenas de usuarios que habían sido sus víctimas. En adición se le exigió que le entregara a su abogado su computadora y equipo relacionado.

Johnson alega ser inocente de las imputaciones de fraude y de dos cargos más sobre abuso a un menor. "Vito" continuó enviando mensajes a sus víctimas aunque sabía que era sujeto de una investigación. "Vito" se ha convertido en un nombre sinónimo de hostigamiento por computadoras que ha aterrorizado a mujeres y niños en varios Estados durante un periodo de dos años.

"Vito" comienza enviando mensajes inofensivos. Luego envía mensajes violentos, hasta que amenaza tanto a la persona con la cual mantiene comunicación como a los hijos de ésta, si ese fuera el caso. "Vito" usó cerca de cincuentiseis nombres falsos y números de tarjetas de crédito alterados para abrir cuentas de uso. No ha sido acusado de acoso computadorizado ya que las autoridades expresan que la ley no atiende adecuadamente el crimen en el espacio cibernético. El vehículo de Johnson tiene una tablilla que lee *Vito Law* (la ley de Vito). Hoy otros acosadores usan el nombre "Vito".[68] Nuevamente la ley es derrotada por el crimen en el espacio cibernético.

8. Pedofilia

Como en la mayor parte de los delitos aquí descritos, no se trata de que sean asuntos nuevos, o de que sea información nueva. La pornografía infantil es una actividad que todos podemos identificar como ilegal, independientemente de que esté en una computadora. Los corruptores de niños entran a la Red fotos pornográficas de niños y las distribuyen ya sea por tablones de edictos electrónicos o por correo electrónico.[69] Como las computadoras son incapaces de diferenciar entre fotos pornográficas y las inofensivas y los mensajes que se dejan adjunto gozan de perfecto anonimato, es muy difícil localizar al responsable de haberlas puesto en exhibición.[70] También se sabe que los corruptores de menores se

[68]Mc Clatchy, *Alt. Internet Media Coverage* (visitado el 28 de septiembre de 1997) <KXTK32B@prodigy.com>.
[69]David Loundly, *E-Law 2.0: Computer Information Systems Operatory Liability Revisited*, (visitado el 20 de agosto de 1997) <http://www.eff.org/pub/legal/e-law.paper>.
[70]*Id.*

contactan unos a otros mediante tablones electrónicos y usan la Red para atraer a menores.[71]

El 4 de marzo de 1992 la policía de Fresno, California contactó a un pederasta homosexual en búsqueda de menores de dieciocho años de edad. Un agente de la policía de aspecto juvenil envió su fotografía y despertó la atención del delincuente. Mantuvieron contacto por semanas, hasta que el pederasta le citó en un restaurante para tomarle unas fotos al desnudo. Cuando se dirigían al automóvil, dos agentes de la policía los detuvieron. Al registrar el cuarto del pederasta encontraron dos videograbadoras, un televisor, una cámara de video, una computadora en cuya pantalla aparecía un cuarto de charla frecuentado por pederastas y cintas de video que contenían imágenes de menores desnudos, muchas de ellas tomadas en ese mismo lugar.

Una semana después de la detención un adolescente llamado Bryan Cox, informó a la policía que él había hecho contacto con el pederasta mediante la Red, que este le había ofrecido darle ayuda con unos problemas técnicos en su computadora. Cuando se encontraron en un restaurante el pederasta se lo llevó a su casa y abusó de él. Forston, el pederasta, fue sentenciado a seis años de cárcel.[72]

El 14 de septiembre de 1995, el Departamento de Justicia de los Estados Unidos, mediante el F.B.I., después de una investigación de dos años sobre el uso de la Red para distribuir pornografía de menores y seducirlos a tener sexo, arrestó a una docena de personas. Esta agencia federal confiscó imágenes digitalizadas de niños, tan pequeños como de dos años de edad.[73] El 29 de diciembre de 1995, *Compuserve* cortó acceso a más de doscientos cuartos de discusión de temas dudosos (bestialidad, sadomasoquismo, rubias) y bases de datos llenas de fotos que se distribuían por la Red. Esto debido a que el gobierno alemán alegaba que *Compuserve* estaba violando la ley al permitir acceso a pornografía infantil.[74]

Este crimen del espacio cibernético tiene un elemento adicional y es que atenta no contra un bien sino contra una persona indefensa que

---

[71] *Id.*
[72] Connie McNamara, *Un corruptor de Menores en el Espacio Cibernético,* READER'S DIGEST SELECCIONES 39-44 (febrero 1996).
[73] Godwin, *Law of the Net: the Wrong Spin,* INTERNET WORLD 86 (enero 1996).
[74] Cortese, *The Internet: Alt. Sex. Bondage is Closed. Should We Be Scared?,* BUSINESS WEEK 39 (15 de enero 1996).

requiere la protección de la sociedad en general. El mundo en el que vivimos hoy es ese mundo que se pensaba para el futuro, donde hasta los niños usan computadoras. Hay que despertar hoy, los niños están expuestos a lo bueno y lo malo de la Red. Un caso que llamó mucho la atención en los Estados Unidos ocurrió en Minoa, Nueva York. Tres niños de trece años de edad, armados con fertilizante, gasolina diesel y planos para hacer una bomba, fueron arrestados por conspirar para hacer estallar su escuela. La policía reportó que otros estudiantes los delataron y así se logró el arresto. En la casa de uno de ellos se encontraron materiales para hacer una bomba. Los planos sobre como hacerla, aparentemente, los consiguieron en la Red.[75]

Hay quienes debatirán alegando que los planos de cómo hacer una bomba pueden conseguirse en cualquier biblioteca, pero la realidad es que niños tan jóvenes de ordinario no acuden a buscar a una biblioteca y cuando lo hacen les parece tan complejo que buscan la ayuda de un adulto. En circunstancias como esa se puede revisar el propósito de la búsqueda que hace el menor. Con las computadoras tiende a ocurrir el fenómeno al revés. Los jóvenes suelen entenderlas mejor que los adultos. Además la industria de las computadoras ha reconocido el interés de los menores por estas máquinas y las preparan para que cada vez sean más fáciles de usar y que cada vez sean utilizadas por niños más pequeños. Muestras de esta tendencia lo son que las compañías de computadoras *Compaq* y la de juguetes *Fisher-Price,* están desarrollando, desde 1996 partes de computadoras como teclados agrandados y controles en forma de automóviles, que harán de una computadora personal un instrumento perfectamente accesible a un niño de tres años de edad en adelante.[76] Niños de tres años de edad podrán usar una computadora, si bien no sabrán leer, quedarán expuestos a las miles de fotografías y gráficas que habitan en el espacio cibernético y que aparecen ante los usuarios con el toque de un botón. Ciertamente los niños están listos para la era de la informática, ¿Serán los adultos capaces de hacer del espacio cibernético un lugar seguro para ellos?

9. Piratería

---

[75] *13 Year Old Boys Arrested in Plot to Bomb School,* THE SAN JUAN STAR, 2 de febrero de 1996, pág. 12.
[76] McWilliams, *Babes in Cyberland*, BUSINESS WEEK 36 (enero 1996).

Se trata de una práctica sumamente común y sencilla. Simplemente requiere que se copie un programa de computadoras de un lado, sea el lugar de trabajo, la escuela u otra fuente y se ponga en un tablón de edictos electrónicos. Cualquier usuario puede accesar uno de estos tablones de edictos electrónicos para exponer lo que desee compartir con otros o copiar, grabar o imprimir lo que otros hayan expuesto en este lugar público.

Los piratas roban programas por muchas razones, desde la ignorancia de la ley hasta razones económicas. La piratería de estos programas hace daño porque ataca el espíritu de la inventiva e innovación. Esto porque se destruye cualquier incentivo financiero que pueda motivar a crear nuevos programas y aplicaciones amenazando el continuo crecimiento de la industria.[77] En el caso *United States v. David La Macchia*,[78] nos encontramos con un típico pirata.

La Macchia era un joven de veintiún años de edad, estudiante del *Massachusetts Institute of Technology* (M.I.T.), quien mediante el centro de cómputos de su universidad preparó un tablón de edictos electrónico llamado *Cynosure*. En el mismo La Macchia animaba a los usuarios a que le enviaran programas de aplicaciones populares como *Excel 5.0* y *Wordperfect 6.0*, además de juegos computadorizados comunes. Una vez se los enviaban los transfería a una segunda dirección oculta *Cynosure II* donde podrían ser copiados por todos los usuarios que tuviesen acceso mediante una clave secreta. La Macchia despertó un intenso interés mundial gracias a la oferta de programas de computadora gratis, inclusive llamó la atención de los oficiales de la universidad y de agentes federales.

Este joven desarrolló un plan para defraudar y facilitar en una escala internacional la copia y distribución ilegal de material de programación con derechos de autor sin pagar licencias o derechos de autor a los creadores y vendedores de los programas. Se estima que esta práctica les produjo pérdidas de más de un millón de dólares a las compañías que tenían los derechos de autor. Aunque La Macchia no obtuvo ningún beneficio económico, se intentó procesarlo por violación al *Wire and Fraud Act.*[79] Como esta ley realmente estaba diseñada para la televisión y

---

[77] SOFTWARE PIRACY FEATURE, *Software Piracy: How to Stay Legal* (visitado el 28 de agosto de 1997) <http://pcnews.com/businessun/features/softwarepiracy.html>.
[78] 871 F. Supp. 535 (1994).
[79] 18 U.S.C. § 1343 (1952).

la radio, el juez estimó que no se había violado esta sección de la ley y que por lo tanto no se le debía tratar como culpable. Aclaró que lo que había hecho La Macchia no era aceptable, pero tampoco era criminal. A raíz de este caso se enmienda la *Ley de Derechos de Autor*[80] que prohíbe el copiar un programa de computadoras para generar ganancias, así como su distribución sin autorización. Contribuye al crecimiento de la piratería de programas el hecho de que este tipo de actividad se considera benigna y no tiene ningún estigma de "acto criminal" ante la sociedad. Tanto individuos, como compañías no le prestan importancia alguna a la práctica de entregar múltiples copias de programas sin tener autorización para hacer las mismas. Como nadie entiende que esto sea malo un treinticinco por ciento de los programas en los Estados Unidos son no autorizados.[81] En Puerto Rico esta práctica es muy común y nadie parece considerarlo ilegal. Ciertamente el daño es severo. En el 1992 la Asociación de Publicadores de Programas rindió testimonio ante el subcomité de Propiedad Intelectual y Administración Jurídica de los Estados Unidos y dijo que los manufactureros de programas de computadoras estaban perdiendo dos punto cuatro billones de dólares de ganancias debido a la piratería.[82] No es para menos cuando consideramos que treintiséis millones de casas norteamericanas tienen computadora.[83]

Este asunto es difícil de controlar, ya que la gente continúa practicando la piratería libremente, y a que a los tribunales se les hace ardua la labor de determinar si ocurre apropiación de la propiedad, la cual requiere que se le quite un bien a otro ciudadano. La dificultad consiste en que puede verse una invasión, pero es muy difícil decir que el pirata asume control físico del derecho de autor. Tampoco se puede establecer que le está quitando al dueño su uso.[84]

La Constitución de los Estados Unidos en su cláusula 8[85] trata sobre patentes y derechos de autor, buscando promover el progreso de las ciencias y las artes útiles asegurando por un tiempo limitado a los autores e inventores derechos exclusivos sobre sus respectivos escritos y descubrimientos disponiendo además que el Congreso tiene el poder

---

[80]17 U.S.C. § 506 (1995).
[81]Davis, *supra* nota 32.
[82]Hornik, *Combating Software Piracy: the Softlifting Problem*, 7 HARV. J. I. & TECH. 377 (1994).
[83]Davis, *supra* nota 32.
[84]Dowling v. United States, 473 U.S. 207, 217-218 (1985).
[85] CONST. U.S. A. art. I, § 8.

exclusivo de promover este derecho. Mientras las compañías continuén amparándose en dicho artículo de la Constitución existirá un alto interés en que se solucione su problema.[86]

10. *Spoofing* o imitadores de sistemas de informática

Spoofing es el acto de disfrazar una computadora para que electrónicamente se vea como otra con el propósito de accesar un sistema al que normalmente le estaría restringido el paso.[87] Al confundir a una computadora que normalmente ofrece seguridad, se puede entrar a otro sistema y este pensará que es una persona autorizada, logrando acceso al mismo y a todo su contenido.[88] El *spoofing* es tan reciente en el espacio cibernético que la misma Red ha tratado de regularlo mediante la creación de varios programas de computadoras que actúan como filtros que neutralizan esta práctica.[89]

Kevin Mitnick, un *hacker* conocido internacionalmente, llegó haciendo *spoofing* a la computadora personal de un destacado proponente de la seguridad en las computadoras. Mitnick dándole una buena llamada de alerta a este experto, robó material relacionado a cómo mantener sistemas de seguridad efectivos y los publicó en un tablón de edictos electrónicos.[90]

11. Traición

Cuando se quebranta la fidelidad, la confianza y la lealtad se ha traicionado. Cuando se traiciona al Estado se le llama a dicho acto alta traición.[91] Cuando se le da vía franca en la Red a un *hacker,* capaz de accesar innumerables centros de información y hasta de entrar a sistemas de los gobiernos, poniendo la información obtenida a disposición de

---

[86]Sony Corporation of America v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984).
[87]Voss, *supra* nota 39.
[88]*Id.*
[89]Joseph Panettieri and Clinton Wilder, *New Net Treat: Filterware Can Protect User From* "*spoofing*" (visitado el 24 de agosto de 1997) <http://techweb.cmp.com/iwk/513/13mtspo.html>.
[90]Voss, *supra* nota 39.
[91]PEQUEÑO LAROUSSE ILUSTRADO, Ediciones Larousse, (9a tirada, 1974) Rue du Montparnasse, Paris.

otros, se tienen los elementos necesarios para que surja traición en el espacio cibernético.

Un grupo de *hackers* compuesto por jóvenes alemanes, denominado el *Club Germán 20*, pensaron que sería divertido entrar a los sistemas de defensa del gobierno norteamericano y del *North Atlantic Treaty Organization* (N.A.T.O.). Pero la diversión se tornó en crimen y traición cuando comenzaron a vender los archivos robados de estas dos instituciones a la Unión Soviética, entre otras naciones orientales.[92]

B. Actos llevados a cabo mediante la Red que podrían catalogarse como delito bajo disposiciones del Código Penal de Puerto Rico

El artículo 107 del Código Penal de Puerto Rico[93] tipifica como delito menos grave las proposiciones obscenas. Este delito está constituido por los elementos de que sea en un lugar público y se haga de manera escandalosa. La intención del legislador cuando redactó esta disposición no pudo incluir el espacio cibernético puesto que este es un mundo descubierto recientemente. No obstante es de conocimiento general para los estudiosos del derecho que las leyes deben ser interpretadas flexiblemente para poder asegurar su longevidad. Siendo los elementos que la proposición obscena sea pública y escandalosa se podría interpretar que si alguien hace proposiciones obscenas en la Red en sus áreas públicas, como lo son los tablones de edictos electrónicos o cuartos de conversación públicos, quedando otras personas sujetas a las mismas, se ha dado este delito, aún en el espacio cibernético ya que se le puede catalogar al mismo como un lugar público.

El artículo 113 del Código Penal de Puerto Rico[94] tipifica como delito menos grave el envío, transportación, venta, distribución, publicación, exhibición o posesión de material obsceno. La persona que envíe, transporte o traiga material obsceno a Puerto Rico para venta, exhibición, publicación o distribución, que lo posea o lo imprima, cumple con los elementos del delito. En el caso de la Red se conoce que esta práctica es cosa de todos los días, que se hace abiertamente, veinticuatro horas al día sin restricciones y miles de puertorriqueños de todas las edades están

---

[92]Ryan Craig and Sergio Chapa, *Crackers and Cracking* (visitado el 28 de agosto de 1997) <http://actlab.utexas.edu/~aviva/compsec/cracker.html>.
[93]33 L.P.R.A. § 4069 (1937).
[94]33 L.P.R.A. § 4075 (1937).

expuestos a la misma. Cuando esta conducta esté dirigida a menores de dieciséis años de edad se está cometiendo un delito grave.[95]

Por otra parte, el Código Penal puertorriqueño en su artículo 117(a)[96] está dirigido a las personas que transmiten material obsceno por televisión, radio o cualquier otro medio electrónico u otro medio de comunicación. Este artículo dispone que quien así actúe cometerá un delito menos grave. Es obvio que la Red podría ser considerada como medio electrónico o de comunicación y por lo tanto constituir un delito de los tipificados por el legislador en el Código Penal.

Por otro lado, el artículo 143, del Código Penal de Puerto Rico,[97] trata como delito menos grave el acto de que una persona se apodere, abra, destruya o suprima cualquier comunicación privada escrita que no le esté dirigida. Cuando se habla de correo electrónico se habla de comunicación escrita, la cual es privada. En esta situación podría surgir una causa de acción contra los criminales del espacio cibernético que practican el *spoofing*. La interrogante es si se podrá extender el término de comunicación privada a comunicación privada electrónica. Igual ocurriría con el artículo 148[98] donde se considera delito grave el que una persona altere en perjuicio de otra el sentido o significado de un mensaje verbal o escrito.

En cuanto a apropiación ilegal[99] para que se logre la consumación de este delito no puede haber violencia o intimidación y se requiere la apropiación de bienes muebles de otra persona. Esta conducta será constitutiva de delito menos grave. Cuando un *hacker* entra y se lleva información de un sistema conectado a la Red ocurre lo mismo, ya que lo esencial es probar que la persona se ha apropiado de bienes muebles que no son suyos. Más específico todavía es el artículo 165(a) del Código Penal de Puerto Rico,[100] donde establece como delito menos grave la apropiación ilegal de propiedad intelectual. Este delito consiste en que una persona copie, reproduzca, imprima, publique, venda o haga copiar, reproducir, publicar o vender cualquier libro, escrito literario, científico o

---

[95] C. PENAL P.R. art. 115(c), 33 L.P.R.A. § 4077 (1937).
[96] 33 L.P.R.A. § 4080 (1937).
[97] 33 L.P.R.A. § 4184 (1937).
[98] 33 L.P.R.A. § 4189 (1937).
[99] C. PENAL P.R. art. 165, 33 L.P.R.A. § 4271 (1937).
[100] 33 L.P.R.A. § 4271a (1937).

musical, pintura, grabado o dibujo, escultura . . . programa o diseño de computadoras o información por métodos electrónicos.

Queda bien claro que la piratería de programas de computadoras o el copiar información electrónica es un delito en Puerto Rico. Este artículo fue revisado en el 1987 y en el 1995 los Estados Unidos enmendaron su *Ley de Derechos de Autor*[101] que prohíbe copiar un programa para generar ganancias, así como la distribución no autorizada de un programa de computadoras. Sin embargo en este estatuto se tipifica como delito grave, así que tenemos un asunto donde se desplaza la ley estatal para que prevalezca la federal, en cuanto a la imposición del grado del delito.

Respecto al escalamiento el Código Penal de Puerto Rico,[102] establece como delito menos grave el que se penetre a construcción o estructura con la intención de cometer apropiación ilegal. En este caso el artículo habla muy claramente de edificaciones, se desprende la intención de proteger estructuras físicas y sería un atrevimiento extender el término al espacio cibernético. Para poder incluir a la Red dentro de este artículo, el mismo necesitaría ser enmendado para que incluyera la penetración por medios de comunicación electrónica a propiedad electrónica con la intención de cometer apropiación ilegal.

Los daños que se cometen contra la propiedad en el espacio cibernético pueden ser vistos a la luz del artículo 179 del Código Penal puertorriqueño,[103] estos aplican tanto a bienes muebles como bienes inmuebles, la pena es de seis meses y basta con que se prueben los daños a la propiedad. Así se puede comprender que al igual que ocurre en el caso de los escalamientos a la Red para hacer daños o en el caso de las bombas a direcciones electrónicas, estos daños podrían ser castigados con este estatuto en observación a lo que ocurre en el espacio cibernético.

La gran dificultad es que ninguno de los artículos anteriores se creó pensando en el caso específico de la Red. Algunos anticiparon la posibilidad de un medio de comunicación electrónico capaz de sufrir los estragos del crimen, pero otros son muy estrictos y jamás contemplaron la posibilidad que hoy es una realidad; crímenes en la Red cuyos efectos están tocando las puertas de los miles de usuarios puertorriqueños. Otro obstáculo para la regulación en la Red es su alcance mundial por lo que se

---

[101] *Id.*
[102] C. PENAL P.R. art. 170, 33 L.P.R.A. § 4276 (1937).
[103] 33 L.P.R.A. § 4285 (1937).

hace difícil controlar a los que participan de ella desde otros países. Los efectos de las leyes de un país terminan con sus tierras y surge un problema de jurisdicción.

C. El asunto sobre jurisdicción en estos casos

Cada vez que ocurre un acto criminal en la Red y las personas envueltas no están en la misma jurisdicción el tribunal tiene que encontrar qué ley puede aplicar. La contestación es más sencilla si todos los envueltos están en la misma jurisdicción o si las leyes de las jurisdicciones son semejantes. Pero cuando la persona de una jurisdicción desea demandar a alguien en una jurisdicción completamente diferente, especialmente si es fuera del territorio de influencia de nuestro sistema, el asunto se complica.

La cuestión de jurisdicción, respecto a leyes penales, es tratada en el artículo 2 del Código Penal de Puerto Rico.[104] El mismo dispone que el Código Penal aplica a todo delito consumado o intentado en el territorio del Estado Libre Asociado (E.L.A.) o fuera de él, si su resultado delictivo se produce en territorio del E.L.A. o por los funcionarios del gobierno del E.L.A. o que lo estén representando en el extranjero. De modo que si algunos de los delitos del Código Penal de la isla se asemejan a los actos que se cometen en la Red y tuviesen sus resultados o fueran planeados en el territorio del E.L.A. se podría procesar efectivamente a un criminal de la Red en los tribunales de Puerto Rico. Pero este asunto no es tan sencillo ya que en los tópicos donde el gobierno federal haya legislado no se puede intervenir y cuando el crimen afecta a varios países, como ha ocurrido, se sigue complicando la ecuación.

En los asuntos de casos relacionados a computadoras, la jurisdicción se ha estado decidiendo de la siguiente forma:

Será según el lugar en que se cometió el acto criminal. En el caso de compañías multinacionales, con centros de operación por el mundo entero, será el lugar de negocios principal del dueño de una computadora, sistema de computadoras o Red. Se toma en cuenta el lugar donde el intruso tenía control de los fondos económicos, archivos, libros, documentos, programas de computadora u otros materiales usados en la violación o muy bien puede ser el lugar desde el cual se logró el acceso a

[104] 33 L.P.R.A. § 3002 (1937).

la computadora.[105] Considerando las leyes de Puerto Rico y las federales se llega a la conclusión de que hay la posibilidad de procesar localmente, pero en el caso de extranjeros que no están en nuestra jurisdicción se dificulta el procedimiento. No cabe duda que solamente con la cooperación activa de cada país es que se puede arrestar y procesar a un criminal con este alcance.

Conclusiones y recomendaciones

A. La posibilidad de un tratado o acuerdo multinacional para una comunidad mundial

Como se ha visto, el crimen cibernético es un problema real, que amenaza con afectar tanto a compañías, gobiernos y ciudadanos. Las leyes en Puerto Rico y en los Estados Unidos no pueden cubrir a la infinidad de ciudadanos que participan de esta comunidad. Existen crímenes y criminales, se ha definido en qué consisten sus fechorías y las consecuencias catastróficas que éstos pueden traer al mundo, inclusive a Puerto Rico. Se ha probado que existe un problema legal, ya que el alcance de las leyes de la isla no puede proteger a todos los usuarios de los criminales en otras jurisdicciones. Se ha expuesto cómo la escasez de leyes realmente diseñadas para enfrentar este tipo de problema ha provocado que nuestros jueces exoneren a quienes cometieron las fechorías a pesar de reconocer que sus acciones fueron deplorables, indicando que no han sido tipificados estos actos como delitos. Por eso hay que buscar alternativas que no sean la mera protección electrónica con instrumentos cada vez más especializados que le compliquen el acceso a los criminales. Es conocido que en ocasiones por más que los usuarios se protejan continúan siendo víctimas y presas fáciles de repetidos ataques una vez se logra entrar a la Red. Esto no se puede permitir, todo ciudadano tiene derecho a ser respetado siempre, nadie debe tomar ventaja de los usuarios, sean personas naturales o personas jurídicas. A su vez los usuarios deben tener la posibilidad de que en caso de un ataque la ley los pueda proteger no importa donde estén.

Una alternativa es que los países entren en un tratado o acuerdo multinacional que establezca una serie de disposiciones legales para la

[105]Otero, *supra* nota 5, pág. 30.

Red. Esto requeriría que los países que participen adopten una cláusula legal multinacional. Este tratado o acuerdo internacional no sería uno sin precedentes. La comunidad internacional ha creado un acuerdo sobre qué ley aplicar a un accidente de tráfico entre ciudadanos de diferentes países.[106] Las naciones del mundo se han puesto de acuerdo en múltiples asuntos, desde cómo tratar a prisioneros hasta el trato de un indocumentado.[107]

El primer paso para establecer una serie de reglas uniformes es identificar alternativas aceptables para todos los participantes y que la misma forme una doctrina legal internacional. Aunque los países sacrifican algo de su soberanía se benefician al lograr un acuerdo sobre jurisdicción y cómo actuar en casos con multiplicidad de ciudadanos, además le ofrecen a los usuarios de la Red seguridad en sus transacciones en el espacio cibernético, sean económicas o no. Se sentirían cómodos al saber que sus asuntos en la Red están protegidos bajo una serie de leyes estables que serán incuestionablemente aceptadas en el mundo entero. Se lograría una manera de procesar a cualquier persona que infrinja estas leyes, aunque sea un criminal en un país extranjero. La Red llega a todas las naciones del mundo, por eso todas deben estar interesadas en cómo será regulada y cómo se gobernará. La Organización de las Naciones Unidas debe dar este paso para identificar los problemas y comenzar por proponer al menos soluciones mínimas para lograr una estabilidad en el espacio cibernético.

B. Puerto Rico ante el crimen cibernético

Puerto Rico aunque tiene un pequeño tamaño territorial, está siempre a la vanguardia. Las telecomunicaciones son parte de la vida del puertorriqueño, el espacio cibernético no es la excepción. Estando ante esta situación es el momento de tomar la iniciativa para proteger a los usuarios locales, sean compañías o individuos. Ya que se ha aprobado la *Ley de Telecomunicaciones de 1996*[108] y ésta establece una Junta para los asuntos relacionados a las telecomunicaciones en Puerto Rico. La misma debe comenzar a identificar los problemas que hay en el espacio

---

[106]ROAD TRAFFIC CONVENTION (Geneva 1949), 3 U.S.T. 3008, 125 U.N.T.S. 22.
[107]46 Stat. 2573, 132 U.N.T.S. 301.
[108]Ley Núm. 213 de 12 de septiembre de 1996, art. 1, 27 L.P.R.A. § 265 *et seq*.

cibernético y sus consecuencias para buscar una manera uniforme de tratar este asunto. En Puerto Rico se debe seguir el ejemplo de los estados norteamericanos y llevar su iniciativa un paso más allá. Se debe hacer un código donde se recojan delitos electrónicos, preparado para incluir las fechorías que ocurren en la Red, a diferencia de los estados de Norteamérica que no contemplan en sus leyes para computadoras el crimen en el espacio cibernético. Esto facilitaría la convicción de infractores y protegería a nuestros jueces de pasar por lo que tantos en los Estados Unidos ya han vivido, el tener que dejar sin amonestación a individuos que claramente cometieron actos negativos, porque las leyes existentes no contemplan la posibilidad del crimen cibernético. Además le daría a las compañías y a los individuos que participan de la Red la certeza de que el espacio cibernético no es tierra de nadie, que hay protección para sus inversiones y que pueden defenderse legalmente de cualquier infractor. Un código de este tipo evita el que las leyes se mezclen confusamente y provee un medio certero y rápido para lidiar con estos problemas.

Esta investigación pudo ser realizada gracias a la Súper Red de Informática. Ya son miles de puertorriqueños los que tienen computadoras en sus casas, oficinas y escuelas. De estas miles de computadoras, cada día un número mayor será conectado a la Red para poder disfrutar de sus ventajas como velocidad, información virtualmente ilimitada y comunicación instantánea con otras personas. Hoy día cientos de los usuarios dependen de su computadora. Por eso es que exigen gozar de cierto grado de protección cuando realizan sus particulares transacciones en el espacio cibernético. El puertorriqueño que se ve limitado por su situación geográfica, ya no lo estará, tendrá acceso, prácticamente inmediato, a personas de cualquier parte del mundo, los negocios disfrutarán de verdadero alcance mundial. Exigirán protección y participación de este nuevo adelanto tecnológico.

C. Respeto hacia la ley en el espacio cibernético, asunto de todos

La autora de este artículo espera que este análisis y exposición contribuya a que el sistema legal del país pueda alcanzarle el paso a la ciencia y a la tecnología. Si las leyes están para proteger a los ciudadanos, entonces las leyes deben proteger a los ciudadanos que conviven en el espacio cibernético. La solución no está en hacer una maraña de leyes que

se entrelacen como una red y que cada vez que hagan falta perdamos tiempo en descifrar cuál de todas se puede aplicar. Cada persona debe velar porque los usuarios respeten a los otros usuarios. Las autoridades pertinentes deben ampliar el significado de las legislaciones actuales, atemperándolas a los cambios que día a día ocurren en el mundo, especialmente el mundo tecnológico.

Si el espacio cibernético es un tipo de comunidad, una urbanización gigante hecha de computadoras unidas alrededor del mundo, entonces parece natural que muchos elementos de una sociedad tradicional pueden encontrarse en forma electrónica. Con el comercio electrónico llegan los comerciantes electrónicos, los profesores "en línea" dan educación electrónica y hay doctores atendiendo pacientes en oficinas cibernéticas. No debe sorprender a nadie que también haya criminales cibernéticos, cometiendo crímenes cibernéticos.[109] Si todos van a convivir en la Red se necesita un cierto grado de protección que asegure que se podrá estar en el espacio cibernético sin temor a ser abusados por los ciudadanos que no respetan los derechos de los demás.

[109]Davis, *supra* nota 32.