

España: Sistemas de Seguridad Informática en la Sociedad de la Información

El diseño e implementación de una política pública de inserción en la sociedad de la información debe contemplar un conjunto de acciones básicas o prioritarias y que deben constituir el núcleo o eje central a partir de los que se desarrolle esta política. Al respecto, pueden existir opiniones dispares sobre lo que debe considerarse una acción básica. A pesar de esta disparidad de opiniones existe una conciencia común sobre la prioridad que debe recibir el fortalecimiento de los sistemas de seguridad informática y su importancia en el desarrollo de una política pública de la Sociedad de la Información.

Si hablamos de seguridad en la configuración de una política pública para la sociedad de la información, lo cierto es que nos encontraremos con diversos problemas a los que se debe poner solución. No obstante, en materia de seguridad, estos problemas presentan sus propias especificidades y ello merece un tratamiento diferente y, en consecuencia, la adopción de medidas diferentes. A continuación, pues, se analizarán los problemas de seguridad y sus posibles soluciones atendiendo a los parámetros relacionados con los derechos de autor, la piratería informática, los contenidos de la red, los peligros de la propaganda ideológica, las garantías para los consumidores y la amenaza de la cyberokupación.

1. Seguridad y derechos de autor

La política pública en la sociedad de la información debe imponer pautas que garanticen el respeto hacia los derechos de autor y la propiedad intelectual y, garantizar, al mismo tiempo, un ambiente de seguridad general en el uso de las nuevas tecnologías.

En cuanto a los derechos de autor, una clara controversia es la que domina el conflicto. Los diversos usuarios de las tecnologías de la información tienen el convencimiento de que todo lo que aparece en redes como Internet puede ser utilizado y transmitido libremente. Pero aunque todo autor desee que su obra sea ofrecida al público y empleada por éste, ello no implica de ningún modo que esté dispuesto a ofrecerla y a consentir el uso libre y gratuito de la misma. Esta situación provoca que exista una auténtica oposición de intereses entre los usuarios de las redes y los autores de sus contenidos.

Actualmente, diversos legisladores nacionales están adaptando sus legislaciones respectivas sobre derechos de autor para proporcionar una protección adecuada a los titulares de estos derechos en cuanto al uso electrónico de sus trabajos.

La protección que ofrece la Ley de Propiedad Intelectual para los medios tradicionales es amplia. Sin embargo, cada vez está quedando más obsoleta o no contempla las “nuevas infracciones sobre la propiedad intelectual”, que pueden cometerse a través de las nuevas tecnologías de la información, añadiéndose a esto la dificultad (o casi imposibilidad) de perseguir a los presuntos quebrantadores de los derechos de autor. La aparición de Internet ha destruido buena parte de las bases sobre las que se apoyaba el derecho tradicional y uno de los casos en los que es más patente esta carencia de normas suficientes para regular nuevas realidades es en la protección de los derechos de autor[i].

Las acciones públicas deben ir encaminadas, pues, a encontrar el equilibrio justo entre proteger los legítimos derechos de quienes crean y seguir encontrando en las redes informativas las ofertas existentes para que los propios usuarios las sigan utilizando.

En algunos círculos jurídicos se ha apuntado la posibilidad de optar por soluciones restrictivas del libre uso de navegación en las redes como por ejemplo en Internet: encriptación de los mensajes o imágenes, mensajes que imposibiliten el acceso mostrando un mensaje de error en la pantalla del usuario no autorizado, etc (Isem, 2001). Sin embargo, tales soluciones drásticas podrían acabar con el éxito del que, al menos por libre acceso, goza la red en la actualidad.

Debemos ser muy conscientes de la necesidad de proteger adecuadamente los derechos de autor en el entorno digital, que son parte de la democracia. El reconocimiento de esta necesidad fue confirmado por 157 estados en el

Preámbulo del Tratado de Derechos de Autor de la Organización Mundial sobre la Propiedad Intelectual (OMPI – ECUP, 1997).

Francia, por su parte, ha decidido emprender algunas acciones que podrían servir para ilustrar a algunos otros países en la cruzada para garantizar la seguridad en el uso de las nuevas tecnologías de la información. Concretamente, el país galo acaba de crear un impuesto especial para computadores y soportes digitales (descodificadores, televisores, teléfonos móviles de tercera generación, reproductores de ficheros de música MP3 y asistentes digitales como Palm). El impuesto aparece con el objetivo de garantizar los derechos de autor frente a delitos como la copia indiscriminada de textos, música y otras obras de autor, que ha aumentado con la implantación de estas nuevas tecnologías[iii].

En este campo de la seguridad y los derechos de autor, seguramente, la estrategia ideal consistiría en crear un marco jurídico para este territorio sin espacio físico concreto. En este sentido, las cláusulas que debería ofrecer toda formulación pública serían las de facilitar, en la medida de lo posible, los mecanismos para que estos avances pudieran producirse.

También podría resultar aleccionador, en el ámbito de las nuevas tecnologías, como ya lo hacen varios portales, incluir en sus creaciones el texto legal sobre derechos de autor, en el que se especifique de quién son los derechos, cuál es su alcance, las condiciones, las prohibiciones y el texto del copyright.

2. Piratería informática

La piratería informática es otro de los aspectos fundamentales que deben erradicarse si se quiere conseguir un auténtico ambiente de seguridad en el universo de las nuevas tecnologías. Básicamente son tres los factores que propician el creciente aumento de la piratería: el progresivo número de internautas, el rápido avance tecnológico y el bajo riesgo de detección del infractor. Estas tres condiciones están generando un enorme mercado sin fronteras para los programas ilegales.

Ya se ha empezado a actuar contra estas actividades pero, sin duda, las políticas públicas en el ámbito de la sociedad de la información deben reforzar las iniciativas que se han tomado hasta el momento. Así, la Business Software Alliance (BSA), entidad que reúne a las principales empresas de software del mundo, ha tomado diversas medidas como el establecimiento de mecanismos de cooperación con los diferentes cuerpos policiales europeos, que han recibido cursos de formación en técnicas y procedimientos sobre piratería informática en Internet.

La importancia de actuar contra la piratería queda explicitada si atendemos a los resultados de un estudio realizado por la propia BSA que indica claramente que la piratería de software es una de las grandes causantes de la caída en el crecimiento de la oferta de empleo en la industria de tecnologías de la información (TI) y de la reducción de impuestos en prácticamente todos los países del mundo.

El estudio se realizó en 61 países. Sólo en Estados Unidos, la piratería impidió que se crearan 140.000 nuevos empleos en la industria del software y que la recaudación fiscal aumentara mil millones de dólares más. En el conjunto de Europa occidental, según la BSA, en 1997, la copia y uso ilegal de programas causó unas pérdidas anuales de 380.000 millones de pesetas.

La propia BSA y la Information Industry Association aseguran que dos quintas partes del software instalado en el mundo es pirata; es decir, el 38% de los 615 millones de aplicaciones de software instalados en el mundo. Además, los países “pirateadores” son los que tienen menos recursos: en Vietnam, la piratería llega al 97%; a continuación encontramos a China, con el 95%, e Indonesia, con el 92%[iii].

La reproducción y venta ilegal de programas informáticos es un problema que afecta a la economía global y contra el que las políticas públicas deberían establecer dispositivos eficaces, mientras los mecanismos legales no aporten soluciones fiables. No obstante, algunos países, como Argentina, ya han reaccionado y han promulgado leyes que convierten a la piratería informática en delito, y pasan a situarse en los primeros lugares de la lucha contra los programas grabados ilegalmente.

3. Seguridad y contenidos en las tecnologías de la información

Al margen de todo lo referente a los derechos de autor o propiedad intelectual se deben establecer mecanismos que proporcionen la protección de los menores y la lucha contra propaganda racista en referencia a los contenidos de Internet. Lo cierto es que hasta el momento los mecanismos para realizar esta lucha son escasos y debe trabajarse duramente para lograrlo. Tan sólo disponemos de algunas acciones o iniciativas que como precursoras pueden marcar el camino a seguir o bien orientar el conjunto de las políticas que deben llevarse a cabo.

En materia de lucha contra el racismo o la propaganda xenófoba en Internet (lo que también se ha venido denominado “odio digital” o “odio on-line”) algunas actitudes que deben seguirse, o al menos que pueden servir de ejemplo, son actuaciones como las del juez francés que decidió emitir un fallo contra Yahoo prohibiendo las subastas, la exhibición o venta de objetos nazis e imágenes racistas a través de Internet.

Alemania, por su parte, uno de los países más dañados históricamente en cuanto a las polémicas y conflictos de identidad cultural así como por la lucha contra la xenofobia, no se ha quedado atrás y con la aparición de una sentencia insta a perseguir judicialmente a los responsables de páginas web con contenidos xenófobos, independientemente del país de origen.

En cuanto a los contenidos que pueden poner en peligro la integridad de los menores destacan las ya lamentablemente conocidas páginas web con uso de pornografía infantil. Tras los escándalos de pedofilia acontecidos en Bélgica, países como Suecia han decidido extremar las precauciones para que este tipo de delitos dejen de producirse, sobretodo a través de las nuevas tecnologías de la información. Un ejemplo claro de esta situación lo podemos hallar en el propio país escandinavo donde Microsoft, tras ser alertada por la policía, tuvo que cerrar una web privada que contenía material pornográfico infantil.

Son muchas las páginas de Internet que distribuyen pornografía infantil y, aprovechándose de la inocencia de los niños, han convertido a la pornografía en uno de los grandes negocios de Internet. Así, resulta fundamental tener en cuenta algunas opiniones como las de la psiquiatra estadounidense Donna Woods, de la Universidad de Michigan, que, en una sesión del congreso anual de la asociación Americana de Psiquiatras, aseguró que se calcula que dos millones de adictos al sexo navegan por Internet en Estados Unidos y que el 20% del comercio electrónico está relacionado con la pornografía.

Esta compleja situación ha provocado que los problemas se vean inmersos en una amplia polémica en materia de ética y derechos humanos. La política americana, basada en la defensa de la libertad de expresión a cualquier precio, empieza a mostrar ya sus flaquezas ante el uso desmedido en algunas de las nuevas tecnologías de la información como Internet, donde se puede encontrar tanto un sitio con contenido científico como uno en el que destacan los materiales pornográficos. Es esta libre distribución de materiales el problema que, por el momento, parece preocupar, en mayor medida, a los legisladores. La polémica entre legislar o no es muy compleja, ya que entre los extremos, ya sean partidarios o no, hay un sinfín de posibilidades. Entretanto, y en referencia a los menores (teniendo en cuenta que la red es usada por más de 10 millones de menores)^[iv], países como el Reino Unido ponen en funcionamiento ciertas propuestas que podrían ser recogidas en el proyecto de elaboración de una política pública en la materia, como la realización de un examen para comprobar si es aconsejable que un menor navegue por Internet libremente. Se sugiere que los menores que pasen dicho examen puedan acceder a los contenidos de la red con menos restricciones que las que actualmente tienen las escuelas primarias. Se piensa que este tipo de test ayudaría a los niños a desarrollar habilidades para responder a personas extrañas que pudieran encontrar en lugares como los populares “chats” y, de esta manera, sacar el mejor provecho de su navegación por la red.

Al mismo tiempo, debemos destacar otra iniciativa emprendida por el gobierno británico para proteger a los niños en edad escolar de los efectos perjudiciales de Internet. Así, las escuelas de Inglaterra están recibiendo del Gobierno británico un paquete de informaciones, que incluye consejos sobre software de filtrado y sobre la utilización de los computadores por menores. La iniciativa también incluye “gridwatch” (“Red de Vigilancia”), un conjunto de orientaciones para los profesores, padres y estudiantes.

En Irlanda, como otro ejemplo interesante, se ha diseñado una línea abierta para denunciar la presencia de material ilegal en la Red. Así mismo, se ha generado una lista de correo, AMSAFE, dedicada a la promoción y discusión de la seguridad familiar en los servicios on line, con el fin de ofrecer un espacio para la discusión entre usuarios y administradores acerca de cómo llegar a garantizar la decencia, integridad, alcance y seguridad al hecho de estar conectado.

Desde la óptica de los proyectos en materia de políticas públicas, mientras no se establezcan innovaciones sustantivas para acabar con este problema, una solución se hallaría en promover los medios para establecer la

posibilidad de construir páginas como las de diversas organizaciones o instituciones que abanderan la lucha contra la pornografía infantil. Una de las más importantes es la de Internet Hottine Providers in Europe (INHOPE).

Otros intentos, como alguno de los desarrollados en California, han intentado crear una red segura para los niños y la familia en Internet. Una de estas iniciativas ha corrido a cargo de la señora St. John que considera que el único sistema para evitar la manipulación de "sitios honestos" es crear otra Internet, algo así como una nueva Internet pero filtrada. Para ello, creó Silvertch que comenzó a crear redes "cerradas" para empresas e instituciones experimentando el sistema Private Internet Engines, similar a unos motores de búsqueda para la Internet privada. Este sistema impide que ingresen los extraños, es decir, quienes no tienen las claves secretas. Su proyecto para los niños "E-kids Internet" sólo incluye contenidos "pedagógicamente irrefutables", basados en la carta de la ONU para los derechos de la infancia. Este proyecto ya tiene casi tres millones de inscripciones gratuitas sólo en Estados Unidos. A pesar de que esta es una iniciativa privada, constituye un buen ejemplo de inspiración de cara a las pautas que deben adoptarse en una política pública.

En materia legal, los Estados Unidos, como hemos visto, uno de los países más afectados en este tema, goza ya de la aprobación de una ley por parte del Congreso que penaliza el uso de Internet cuando se implica a menores de 18 años en actividades sexuales o para enviar o recibir pornografía infantil. La ley establece multas y penas de cárcel para quienes ejerzan actividades delictivas de este género. Esta ley fue reforzada con un acuerdo entre el Congreso de Estados Unidos y la Casa Blanca para desarrollar otras leyes que limitaran el acceso de los niños a los websites con contenidos pornográficos así como para aprobar de un presupuesto por 500.000 millones de dólares para proteger a los niños de la pornografía en Internet. En esta misma línea, el ya ex-candidato a la presidencia de los Estados Unidos, Al Gore, pidió al Congreso, durante el ejercicio de su vice-presidencia, la agilización del estudio sobre una ley para exigir a las escuelas y bibliotecas, que reciben subsidios federales para desarrollar el acceso a Internet, instalar filtros que bloquearan el material inadecuado para los menores.

De otro lado, debemos destacar que algunas instituciones se han reestructurado para luchar contra los contenidos que aparecen a través de las nuevas tecnologías de la información. Este es el caso de la Internet Watch Foundation (IWF). Esta institución participará en la creación de un plan de filtrado internacional para proteger a los niños de los contenidos considerados perniciosos a través de la Internet Content Rating Association. Así mismo la IWF también quiere acabar con el racismo en Internet usando un acercamiento autorregulador.

La imitación de esta estrategia, por parte del resto de gobiernos a escala mundial, podría ser un buen inicio con el que empezar a dar respuestas sólidas a los problemas de contenido en las redes digitales.

Europa, por su parte, no ha querido quedarse atrás y la Unión Europea, a finales del pasado año 2000, lanzaba una convocatoria para financiar proyectos que tuvieran la finalidad de evitar los contenidos nocivos en Internet. Este llamado, que abarca convocatorias y servicios de filtrado, forma parte del plan de acción para propiciar una mayor seguridad en Internet. Así, esta iniciativa constituye un buen ejemplo a seguir a la hora de recoger, en una futura política pública de la sociedad de la información, cláusulas para garantizar la seguridad de las redes y luchar, así contra los contenidos nocivos que circulan en ellas[v].

Decantar una iniciativa pública hacia los sistemas de filtrado supone tener en cuenta una serie de inconvenientes: estos filtros no abarcan el total de sitios web y muchas veces sus criterios de selección son equivocados. Por tanto, se reclama un tratamiento claro, preciso y uniforme de las informaciones clasificadas, de manera que cualquier usuario sea advertido de su contenido. Las decisiones limitativas deberían ser adoptadas por las personas en el uso de la responsabilidad, como padres y educadores, y nunca por instituciones ajenas.

Una buena estrategia a seguir es la disponibilidad de líneas abiertas para denunciar la presencia de material ilegal en la Red, como sucedió en Irlanda. Al mismo tiempo, se propone la posibilidad de incluir logos en las páginas web en los que se enuncie que una página es segura para toda la familia. Más propuestas en este ámbito, son los deseos de designar una terminación ".adult" con la que se advierta que esta página es para adultos, junto con un "chip" especial que permita filtrar las páginas que los padres quieran mantener lejos de sus hijos.

Por su parte, diversas organizaciones como "Hackers contra la pornografía infantil" (EHAP) también han empezado a reaccionar y están empleando la tecnología para descubrir la identidad y la localización física de las personas que envían pornografía infantil a los newsgroups, salas de chat y sitios web. EHAP, formada por ingenieros y profesores de informática, pasa la información a las agencias policiales. Estos lazos de colaboración deberían fomentarse a través de las diversas iniciativas que pueda comprender una política pública de la sociedad de la información en la materia.

“CyberAngels” también es una red internacional de usuarios de Internet que ofrece consejos y ayuda a las agencias de seguridad para luchar contra la pornografía en línea.

Una de las causas por la que estos tipos de delito siguen creciendo se debe a que muchos sitios web, proveedores y otros usuarios de Internet, que habitualmente recogen datos personales de jóvenes y niños, no notifican a los padres acerca de ello. Ante esto se aconseja que se exija a los sitios web la obtención del permiso paterno antes de recoger datos de los menores como nombre, dirección de correo electrónico y postal, teléfono, edad, etc.

Todos los inconvenientes destacados no deben hacernos olvidar también los problemas que las nuevas tecnologías de la información, a nivel de contenido, han presentado en aspectos como el de la discriminación de las mujeres. Las políticas públicas en la materia deberían imitar estrategias como las adoptadas por la ONU, que se apoyó en Internet para llevar a cabo una campaña para combatir la violencia contra las mujeres. Con esta iniciativa, más de 1.300 mujeres y hombres del mundo militaron contra la violencia y se comunicaron por correo electrónico durante meses, comparando experiencias y compartiendo estrategias de lucha contra la violencia de género[vi]. Otra página a tener en cuenta en este ámbito es la de la Agencia de Naciones Unidas en Latinoamérica y el Caribe, que promueve la campaña “Una vida sin violencia es un derecho nuestro”.

Si bien con una clara orientación ideológica, gobiernos dictatoriales o semi-dictatoriales, como los de China o Cuba, están iniciando programas de control sobre los contenidos que aparecen en las nuevas tecnologías de la información; si bien el objetivo no es imitar tales iniciativas, sería interesante observar con más detalle qué procesos de filtrado emplean para evitar los contenidos que, en su opinión, pueden acabar resultando nocivos. Uno de los casos a observar lo tendríamos en China donde el Ministerio de Seguridad Pública creó un programa de computación para mantener fuera de Internet a “los cultos, el sexo y la violencia”. El programa INTERNET POLICE 110 fue lanzado para impedir a los usuarios acceder a cierto tipo de información de sitios extranjeros y del país. El programa, disponible en versiones diferentes para hogares, cafés Internet y escuelas, puede vigilar el tráfico en Internet y bloquear mensajes de fuentes consideradas ofensivas.

4. Propaganda ideológica

Otro de los delitos que empieza a ser ya habitual en el uso ilegal de las nuevas tecnologías se basa en la presencia de manifestaciones ideológicas, normalmente de carácter político, en algunas de las páginas de Internet de organismos oficiales, partidos políticos o entidades institucionales. Básicamente, este conjunto de delitos es llevado a cabo por activistas motivados por razones políticas y sociales que acaban constituyendo una nueva variedad de criminal cibernético.

Diversos países han sufrido ya sus ataques sin que se haya podido solventar el problema al instante o bien prever su actuación. Por ejemplo, la página del gobierno de Chile sufrió el ataque de un grupo de “hackers” autodenominado “ex legumbres asesinas mutantes de Marte” que criticaban a la clase política y alentaban al presidente Ricardo Lagos a combatir la pobreza y la delincuencia en el país.

También destacan casos como el de Malasia, país cuya página parlamental vivió el ataque de un grupo de delincuentes cibernéticos que eliminó toda la información.

Otros ejemplos ilustradores de estos casos los podemos encontrar en Perú donde las páginas en Internet de la Oficina Nacional de Procesos Electorales (ONPE) y del Jurado Nacional de Elecciones del Perú (JNE) fueron retiradas sorpresivamente del ciberespacio, al parecer, debido a un ataque de piratas informáticos que llenaron ambas portadas con mensajes en lengua portuguesa.

Así, también la página de la AIPAC (American Israel Public Affairs Committee) fue atacada el pasado 6 de noviembre de 2000 por un hacker pro palestino llamado doctor Nuker. La página fue desconfigurada, con lo que obligaba a la AIPAC a clausurar temporalmente su presencia en la red. El malestar que se vive en Oriente Próximo parece ser el responsable de los ataques cibernéticos entre los simpatizantes de uno y otro bando. Los objetivos conocidos incluyen páginas puestas en marcha por el gobierno civil y militar israelí, así como aquellas gestionadas por organizaciones a favor de la causa palestina, según el Centro Nacional de Protección de Infraestructuras (NIPC).

Y si bien hemos citado estos ejemplos, la lista sería bastante más larga, y es que los ataques a las diversas páginas nacieron casi al mismo tiempo que Internet. Así, tampoco se han salvado de los ataques la página del New York

Times, las de organismos oficiales de países como Turquía, la India o Pakistán y las de otras organizaciones como la CIA o el FBI.

Todo este conjunto de sucesos está acabando de consolidar lo que ya se conoce como la “Guerra de la Información” o “Infoguerra” (“Information Warfare”).

Para acabar contra esta “infoguerra”, si bien tecnológicamente las innovaciones no son destacadas, sí lo es la postura ante el problema así como la actitud a demostrar para poder encararlo. Así, en la VII Asamblea Anual del Foro Parlamentario Asia Pacífico, en la que participaron delegados parlamentarios de más de 20 países, se propuso el rechazo internacional de cualquier tipo de propaganda subversiva o terrorista difundida a través de la Red.

Una de las consecuencias de esta “infoguerra” ha sido la creciente preocupación, en los últimos años, por la posibilidad de un ataque cibernético de carácter bélico a los centros de información militares y políticos del país. De tener éxito, un ataque de estas características podría inutilizar los sistemas de decisión política y de respuesta militar del país agredido y, por lo tanto, podría dejar al país a merced de cualquier agresión externa.

Si atendemos a algunos de los sucesos acaecidos en los últimos tiempos, la guerra en el ciberespacio no parece ser una mera hipótesis de las muchas que se barajan en las jefaturas militares de las grandes potencias, sino que ya es un hecho. Esto parece indicar la actividad que se registra en Taiwán, país que durante el mes de febrero del año 2001 recibió 80.000 “ataques” provenientes de China continental. Así lo señala el primer informe oficial publicado en la isla sobre la ciberactividad bélica entre ambos lados del estrecho de Taiwán.

El informe indica que en los últimos cuatro años se han registrado 250.000 “ataques premeditados” de ciberpiratas del continente. Estos ataques están dirigidos a las redes informáticas de los organismos gubernamentales, en especial de defensa, y parece que, en los últimos meses, se está llegando incrementando tanto en el número de ataques como la magnitud de destrucción y la peligrosidad de estos.

Además, se calcula que el número de ataques reales es mucho mayor que el de las cifras oficiales. Según se puede inferir de los contenidos de los ataques, éstos tienen como objetivo fundamental la destrucción de la red vinculada a los sistemas de defensa. Por lo tanto, parece que estos ataques obedecen a una “ciberguerra” bien planificada por expertos.

Este nuevo uso perverso de la Red, nos indica que estamos entrando en un nuevo estadio de la historia en el que las nuevas tecnologías se emplean como medio de acceso para destruir los sistemas informáticos de los países que puedan ser considerados como “enemigos”.

Así pues, aunque no es un objetivo prioritario dentro de las acciones a emprender, convendría que aspectos como éste no pasaran desapercibidos y entraran dentro de un campo de consenso internacional con el fin de programar acciones y proyectos que impidan este tipo de actividades encauzándolas más hacia un desarrollo social y benéfico de la red.

5. Garantías para los consumidores

A pesar de las categorías que hemos destacado previamente, lo cierto es que los delitos predominantes a través de las nuevas tecnologías de la información son aquellos que podemos considerar como los “tradicionales”, que comprenderían toda la galería de estafas y “timos” que pueden llevarse a cabo electrónicamente. Así, las redes de la información son propicias para extender amplias innovaciones delictivas como el fraude a través de tarjetas de crédito, la intrusión en las redes de empresas y administraciones públicas, los virus informáticos, las falsas oportunidades de negocio, los engaños en vacaciones y viajes o la piratería de programas.

Al mismo tiempo, aparecen nuevas formas de negocio que escapan de los cauces legales como la novedosa venta ilegal de medicamentos a través de Internet. Así, la Junta Nacional Internacional de Fiscalización de Estupefacientes (JIFE), un organismo de Naciones Unidas (ONU), advierte en su informe anual que las farmacias que operan en Internet proporcionan de forma ilegal medicamentos que requieren prescripción médica a clientes de todo el mundo, sin exigir la receta correspondiente. La agencia de Naciones Unidas insta a los Gobiernos a que elaboren legislación específica y colaboren a nivel internacional (un buen aspecto que debería recogerse y promocionarse en las iniciativas públicas) para aplicar controles estatales que eviten estas prácticas. Así, deben establecerse cauces de

cooperación para que los gobiernos establezcan mecanismos para elaborar normas jurídicas comunes en esta esfera y coordinar las actividades de sus autoridades de represión contra el uso ilícito de Internet.

En estos aspectos, las diversas iniciativas legislativas se encuentran en pleno período de avance, demostrando que no están adaptadas a la nueva realidad, en la que son comunes los delitos transnacionales que no tienen un domicilio concreto ya que se realizan a través de redes como la de Internet. A esto, podemos sumar que las denuncias “on-line” aún no tienen validez legal y para ello será necesario que previamente los jueces acepten la validez de la firma digital para las denuncias a través de Internet.

El proceso de firma digital avanza progresivamente. El mes de julio del pasado año, el ya ex-presidente norteamericano Bill Clinton aprobaba la ley de firma digital que otorga la misma validez de las firmas tradicionales a las firmas electrónicas. Este paso, para aumentar la seguridad de la red, ya ha sido dado en otras zonas del mundo como la Unión Europea, y en países como España (a través del Real Decreto sobre Firma Electrónica) y Argentina[vii]. Es previsible que esta legislación se extienda rápidamente para hacer frente a los retos que representan los espacios virtuales sobretudo en los campos que hemos visto. Además, se convertirá en un instrumento clave para la certificación en el sector público : las administraciones podrán utilizarlo para tramitar documentos internos y con los ciudadanos, para contratos públicos, afiliaciones a la Seguridad Social, atención sanitaria, etc. Se aboga que sean los gobiernos los responsables de ofrecer y controlar los servicios de firma electrónica y digital incentivando, de esta manera, el aumento de transacciones virtuales y haciendo desaparecer, así, la desconfianza que aún mantienen muchos usuarios al respecto, garantizando la identidad de las partes y haciendo confidenciales los datos.

Por otro lado, debemos ser conscientes de que la protección de contenidos es difícil (además, existe la tendencia que nos indica que a medida que aumentamos los niveles de seguridad, se incrementa el riesgo para el contenido, ya que aumentan los incentivos y la voluntad de los “hackers” por violar cualquier nueva creación)[viii] y de que los micropagos son poco rentables si no se emplea un sistema adecuado (por ejemplo, pagar 20 pesetas con una tarjeta VISA es ruinoso para todas las partes). Además, en algunos países en vías de desarrollo, como los de la región latinoamericana, no existe una cultura de tarjeta de crédito, por lo que intentar establecer mecanismos de pago a través de ella puede ser totalmente infructuoso.

Todo el conjunto de países vinculados al avance de las nuevas tecnologías es consciente de la dimensión que toman estos delitos y de la necesidad de actuar de un modo rápido antes de que el problema pueda estar fuera de cualquier control. Por este motivo, países punteros en el campo de la sociedad de la información, como Estados Unidos, han decidido no dejar pasar más tiempo y empezar a proporcionar mecanismos de lucha contra la variedad de delitos que hemos visto. Así, se ha creado el “Escuadrón Nacional de Alta Tecnología” que empezó a funcionar a partir del mes de abril del presente 2001. Este cuerpo está integrado por 80 ciberpolicías que intentarán coordinar los esfuerzos para que todas las agencias judiciales puedan compartir información sobre crímenes electrónicos registrados en este país.

Y ya que hemos citado a los Estados Unidos, no podemos olvidar tampoco una de las iniciativas fundamentales que se han tomado en el país para proteger la privacidad de los usuarios en referencia al conjunto de datos personales que podrían estar circulando por la red en este momento. Así, la Asociación Electrónica de Estados Unidos ha solicitado al gobierno que establezca reglas sobre el uso de los datos recolectados por las empresas a través de Internet y presentó las características que debería tener una legislación para proteger a los consumidores. Esta preocupación está justificada de antemano, pero se incrementa si tenemos en cuenta la posibilidad de que muchas empresas de Internet hayan podido vender sus bases de datos de clientes para afrontar los problemas derivados de los diferentes momentos de crisis económica. La asociación, de 3.500 miembros, dijo que prefería que la recolección de datos por Internet estuviera regulada por un conjunto de leyes federales en lugar de variadas y eventualmente contradictorias disposiciones de los estados[ix]. Este caso, pues, constituye un nuevo ejemplo a seguir y determina que las políticas públicas, en este ámbito, posibiliten la oportunidad de que diversos organismos y asociaciones colaboren conjuntamente con los poderes públicos para afrontar esta clase de graves problemas.

Algunos países, como México, han decidido seguir la estela de los Estados Unidos y, en este caso, el país latinoamericano anuncia que, a través de la Procuraduría Federal del Consumidor de México (PROFECO), se podrá intervenir en caso de que tiendas o proveedores falten a las promesas de venta o no proporcionen información en la página web. La PROFECO reconocerá las quejas de los consumidores de Internet e intentará establecer reglas para evitar que los comerciantes on-line puedan engañar a los clientes. Las reglas que deben seguir tiendas y proveedores son:

- Cumplir con lo que ofrecen.

- Dar a conocer a sus clientes exactamente los cargos por envío o adicionales.
- Explicar, con detalle, en qué consiste el bien o servicio que proporcionan.
- Garantizar transacciones seguras.
- Explicar si sus productos afectan a cierta población vulnerable.

Éste es un buen ejemplo, pues, del tipo de organismo que en toda política pública de la sociedad de la información se debería promover con la intención de garantizar la seguridad de los usuarios en sus transacciones a través de las nuevas tecnologías de la información.

España, por su parte, inició en 1999 el camino para garantizar la seguridad electrónica en este ámbito y puso en funcionamiento un centro para perseguir delitos económicos en Internet (dependiente de la Agencia Tributaria).

Y aunque los países empiezan a desarrollar sus propias estrategias de combate contra los problemas de seguridad, algunas iniciativas de carácter internacional también han prosperado y merecen ser tenidas en cuenta. Así, quince bancos de once países del mundo, que representan a más de ochocientas entidades financieras, constituyeron una agencia global (GTA – Global Trust Authority) para garantizar la seguridad de las transacciones y del comercio electrónico a través de Internet. Para ello, este nuevo organismo dictará los requerimientos que deberán cumplir los organismos emisores de certificados digitales. En este sentido, a pesar de tratarse de una iniciativa privada es un buen ejemplo del éxito que podría lograrse en caso de llevar a cabo una iniciativa pública de semejantes parámetros.

6. “Ciberokupación”

Uno de los problemas que no deben descuidarse a la hora de plantear una política pública de la sociedad de la información en materia de seguridad es el referente al reciente fenómeno de la “ciberokupación”.

En esencia, el fenómeno o, más bien problema, de la ciberokupación surge en el momento en que diversos internautas (conocidos ya como “ciberokupas”) registran nombres de dominio de empresas de modo que, cuando éstas pretenden registrarse para figurar en Internet, se encuentran con que su nombre ya está ocupado. De este modo, si quieren recuperarlo deben pagar una alta suma de dinero a la persona que se les adelantó.

Este problema afecta a varios países del mundo y, si bien quizá no es uno de los ámbitos prioritarios a tratar en materia de seguridad, su creciente extensión determina que la problemática no deba pasar desapercibida. Entre los países más afectados se encuentra España, que fue el tercer país más denunciado por delitos de este tipo ante el sistema de arbitraje puesto en marcha a finales de diciembre de 1999 por la Organización Internacional de la Propiedad Intelectual (- OMPI -, organización de carácter intergubernamental, dentro de la estructura de Naciones Unidas, con sede en la ciudad suiza de Ginebra, con 173 estados miembros[x]), para resolver disputas por el uso abusivo de dominios de Internet.

En total, ante el centro de Mediación y Arbitraje (CMA) de la OMPI se han presentado denuncias contra 1.045 personas de todo el mundo, 64 de las cuales residen en España. La lista de países más demandados está encabezada por los Estados Unidos, con 568 denuncias, seguido del Reino Unido, con 79. Por detrás de España se sitúan Canadá (39), Australia (28), la República de Corea (24), Suecia y China (21) y Francia (18).

En cuanto a los países que más demandas han interpuesto ante el CMA, España ocupa el cuarto lugar, con 56 denuncias, por detrás de Estados Unidos (528), Reino Unido (95) y Francia (64). Los residentes en Alemania siguen de cerca a los españoles con un total de 32 denuncias; a continuación encontramos a los suizos con 29 y los australianos con 27 (El Mundo, 2000).

Hasta el momento, no existe ningún tipo de medida o precaución que se dedique a prevenir estas acciones y este aspecto no debería pasar desapercibido ante la posibilidad de realizar una política pública en la sociedad de la información. Así pues, los únicos procedimientos existentes son de carácter reactivo y se desarrollan, exclusivamente, por los cauces de la vía judicial. El procedimiento formal trata de encontrar soluciones en un período de 45 días, en los que el tema es estudiado por un grupo de uno a tres especialistas designados por la OMPI. Los casos más complejos quedan en manos de los tribunales.

Por su parte, es la política de la Corporación de Asignación de Nombres y Números de Internet (ICANN)^[xi] la que establece el marco jurídico para la solución de las controversias existentes entre el titular de un nombre de dominio y un tercero (es decir, una parte distinta a la del titular) por el registro y utilización abusivos de un nombre de dominio de Internet. Esta política, aprobada en las reuniones celebradas el 25 y 26 de agosto de 1999 (los documentos de ejecución fueron aprobados, posteriormente, el 24 de octubre del mismo año) en Santiago de Chile por la Junta Directiva de la ICANN, se basa ampliamente en las recomendaciones contenidas en el Informe de la OMPI sobre el proceso relativo a los Nombres de Dominio en Internet. En este sentido, cabe destacar que todos los registradores de dominios de Internet acreditados por la ICANN que están autorizados a registrar nombres en los dominios de nivel superior (.com, .net o .org, por citar algunos) han aceptado someterse a la política de la ICANN y ejecutarla. Así, cualquier persona o entidad que desee registrar un nombre de dominio en los dominios de nivel superior está obligada a aceptar las cláusulas y condiciones de la política de la ICANN.

La mayor parte de empresas implicadas en disputas de “ciberocupación” prefieren someterse al arbitraje por ser éste mucho más económico que la decisión de un pago millonario, o por no poner en marcha el aparato judicial, debido a los costes y el tiempo que conlleva tal proceso. Aproximadamente el 83% de las demandas presentadas ante la OMPI se resuelven a favor del demandante, cifra elevada si se compara con los arbitrios de “eResolution”^[xii], que tan sólo resuelve un 49% de los casos a favor de los demandantes.

No obstante, a pesar de estas indicaciones que pretenden dar muestra de un gran control y una robusta seguridad, lo cierto es que los delitos de este tipo siguen produciéndose progresivamente. Además, a nivel mundial, no existe un consenso por parte de los diversos países y, en función del caso que estudiemos, un país determinado puede presentar medidas más severas que otro, lo que hace que casos similares tengan soluciones diferentes. En esta situación, deberían promoverse actuaciones, proyectos o programas que trataran de buscar el acuerdo entre países ante un problema que les afecta de una manera similar pero que recibe trato diferente en los tribunales (por ejemplo, la jurisdicción es mucho más severa en países como España o Chile que en otros como Argentina).

Como mecanismos alternativos al problema han surgido diversas empresas especializadas que tratan de buscar marcas o soluciones para clientes cuyos dominios han sido ocupados. No obstante, soluciones de este tipo no son una vía de escape totalmente fiable si tenemos en cuenta que las posibilidades de encontrar dominios son cada día más escasas, ya que éstos se agotan cada día más (nos encontramos ante un fenómeno que ha sido incluso etiquetado como “la guerra de los dominios”) y que al hablar de política pública no se puede seguir la vía de iniciativas privadas como ésta.

De acuerdo con lo que indicábamos en el párrafo anterior, actualmente, es casi imposible encontrar un dominio .com correspondiente a alguna palabra en inglés que no haya sido utilizado por nadie. Un estudio realizado por Names Direct refleja que la angustia por encontrar nombre ha hecho que se agoten todas las palabras en inglés. Según el estudio, todas las combinaciones de tres letras y tres números se agotaron en abril y los nombres comunes son muy escasos (Castañeda, 2001).

La llegada masiva de las empresas a la red y el crecimiento exponencial de usuarios han hecho que cada vez sea más difícil llamar con nombre propio al alojamiento. Ya hay registrados 9.482.427 dominios “.com” y 17.738857 dominios “.org”, “.net” , “.gov” en todo el mundo.

Ante esta situación, como posible pauta de solución, ha empezado a nacer un nuevo fenómeno en la era de la sociedad de la información: los bancos de dominios. Con base de operaciones en Jerusalén, se presentaba el primer banco de inversiones mundial para nombres de dominio en Internet: “GoldNames”. Esta entidad se dedica a proveer a las compañías de Internet de nombre para dominios de “alta calidad” y, lo más importante, que aún no estén registrados. No obstante para nuestro caso este tipo de resoluciones no constituyen un buen modelo de inspiración teniendo en cuenta que se trata de iniciativas privadas.

7. Algunas medidas generales

Tras lo visto, podemos concluir que, en líneas generales, la política pública en materia de seguridad electrónica, debe procurar tener incidencia sobre estos aspectos :

- Acceso : Se deben establecer mecanismos para controlar (o limitar) quién puede acceder al contenido, si bien ello puede reducir el atractivo que hasta el momento tenía la posibilidad de navegar libremente por Internet.

- Seguimiento : Determinar qué han hecho los usuarios con el contenido. Esto puede ser aún más complejo y, llevado al extremo, podría causar problemas de invasión en la esfera privada de los ciudadanos.
- Pago : Gestionar la recepción de la cantidad estipulada por el uso del contenido. Pero también debemos tener en cuenta que pagar por todas y cada una de las consultas o usos de los materiales sería excesivo y, nuevamente, reduciría , de modo considerable, las ventajas que, en este momento, nuevas tecnologías como Internet nos aportan.
- Regularizar, avanzar y consolidar todos los procesos relativos a la firma electrónica y la firma digital.

Al mismo tiempo, la mayor parte de políticos del mundo coincide en que no es posible una lucha efectiva contra el cibercrimen sin un marco legislativo global que impida que los delincuentes puedan refugiarse en paraísos cibernéticos. Así, la regulación jurídica debe correr paralela a las diversas iniciativas o avances que se emprendan en la materia para lograr conseguir resultados beneficiosos y que, además, tengan amparo en la ley. La Unión Europea está trabajando, en este sentido, en el marco territorial de los Quince.

A pesar de que puedan encontrarse diversas soluciones de carácter puntual, como las que han sido indicadas, es absolutamente necesario desarrollar un marco normativo y legal que comprenda todo el conjunto de delitos que hemos ido señalando, especificando qué se entiende por delito, sus posibles castigos así como las diversas estrategias que deben ser desarrolladas para prevenir o paliar estas situaciones tan conflictivas.

Esta es una premisa ineludible que toda política pública de inserción en la Sociedad de la Información debe tener muy en cuenta y sin la cual es muy difícil avanzar en el uso de las nuevas tecnologías de un modo beneficioso para las naciones y sus respectivas poblaciones. No obstante, los avances son lentos y complejos y, por el momento, no podemos destacar una creación lo suficientemente significativa y eficaz ante los retos y dificultades que en este punto hemos planteado.

Referencias

Castañeda, J. "La fiebre de los dominios". Baquía Internacional. 12 de marzo. 2001.

ECUP. "Por una Sociedad de la Información equilibrada". Diciembre. 1997.

El Mundo. "España, el tercer país que más sufre la ciberokupación". 21 de marzo. 2000.

Isern, M. "Ciberespacio y Propiedad Intelectual", mensaje nº 10, Infonomía, 17 de enero del 2001.

[i]Según el artículo "¿ Cómo proteger los derechos de autor de sus creaciones intelectuales publicadas en Internet ?", Revista de Derecho Informático (ALFA-REDI), <http://www.alfa-redi.org/publicacion/>

[ii]Tal y como aparece en "La Vanguardia", 16-01-2001.

[iii] Según "La propiedad intelectual en la era de los bits", Servicio de Información sobre Internet.

[iv] Según "Hackers y Cyberangels", Servicio de Observación de Internet (SOI)

[v] Debemos destacar en este aspecto que varias compañías ya se han movilizado para crear estos filtros y sus avances pueden constituir una buena pauta de inspiración para la inclusión de sus estrategias en una política pública. Así, NetNanny es un programa de control de contenidos y CyberPatrol restringe las horas de uso de Internet. También Inktomi , uno de los desarrolladores de tecnología de búsqueda de la Red, se acaba de asociar con el fabricante de bloqueo N2H2 para desarrollar un masivo índice de la Red para adolescentes que excluirá enlaces a contenidos pornográficos.

[vi] según comentarios de Noleen Heyzer, directora del Fondo de las Naciones Unidas para la Mujer (UNIFEM), en: <http://revistaldesur.org.uy/revista.092/ciberzoo1.html>

[vii]Dónde se implantó en la Administración Pública, empleando, desde 1998, esta tecnología para los actos internos del Sector Público que no produzcan efectos jurídicos individuales en forma directa, y ha sentado las bases para la creación de la Infraestructura de Autoridades Certificantes de la Administración Pública Nacional

[viii] Básicamente, a medida que se aumentan las condiciones de seguridad los hackers se ven impulsados a violarlas ya que esto les concede un mayor prestigio dentro de las comunidades hackers. La violación de sistemas

más seguros constituye una muestra de su pericia y habilidad, lo que les reporta un respeto por el resto de hackers convirtiéndose, muchas veces, en personajes admirados o imitados por el resto.

[ix] Según Reporters Online, 19-01-2001.

[x] al menos hasta el 17 de diciembre de 1999 según “Procedimientos contra la ciberokupación”, en http://www.todoiure.com.ar/monogr.../derecho_e_internet2.ht

[xi] Se trata de una corporación de carácter no lucrativo.

[xii] Consorcio acreditado por ICANN el 1 de enero del 2000 como organismo proveedor de soluciones en caso de disputas por nombres de dominio.

Oscar del Alamo
