La prevención del ciberdelito

Fernando Miró Llinares

PID_00195952

Universitat Oberta de Catalunya

Índice

Introducción

El conocimiento y análisis del fenómeno de la criminalidad debe ir ligado a la búsqueda de soluciones que evite la comisión delictiva o, por lo menos, reduzca la incidencia, así como minimizar sus efectos dañinos para la sociedad. Por eso, el presente módulo está pensado para que el estudiante conozca diferentes estrategias de prevención de la cibercriminalidad.

Para ello, el módulo se ha divido en cuatro apartados siguiendo una estructura lógica de analizar primero el ámbito en el que se produce la ciberdelincuencia a través del análisis de las características que lo definen. Después se estudiarán los comportamientos que inciden en el proceso de victimización. Y por último, se estudiarán teorías aplicadas al fenómeno de la cibercriminalidad así como distintas estrategias de prevención.

Objetivos

En los materiales didácticos de esta asignatura, el estudiante encontrará las herramientas básicas para alcanzar los objetivos siguientes:

1. Conocer cada una de las características que conforman el ciberespacio.

2. Adquirir conocimientos sobre la importancia del actuar de la víctima en proceso de victimización.

3. Familiarizarse con los distintos enfoques de las teorías de la criminalidad aplicada al cibercrimen.

4. Aprender a establecer estrategias de prevención.

1. ¿Cómo prevenir el ciberdelito?

Vivimos en la sociedad de la información caracterizada porque son las TIC las que impulsan múltiples cambios tanto sociales como políticos y económicos. La suma de evoluciones tecnológicas en el campo de la microelectrónica, la informática y las telecomunicaciones, entre otras, junto a la aparición del paradigma de innovación tecnológica que ha supuesto una mayor incidencia social, como ha sido Internet, que ha vuelto los mercados financieros transfronterizos, multiplicado las opciones de acceso a información de todo tipo, permitido transacciones económicas o personales transfronterizas y en tiempo real, creado nuevas formas de comunicación personal y modificado los contextos y sentido de cualquier forma de comunicación; ha provocado múltiples cambios en lo económico, cultural y social.

Ante la realidad de la existencia de la cibercriminalidad, el siguiente paso lógico es plantearse cómo se puede prevenir este tipo de delincuencia. Para llegar a este punto será necesario plantearse diferentes cuestiones a las que iremos dando respuesta conforme vayamos avanzando en el tema:

- En primer lugar, Internet como red global ha supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica, que se ha denominado **ciberespacio**, y respecto al cual nos interesa plantearnos si el mismo puede definirse como un **nuevo ámbito de oportunidad delictiva**, un contexto de riesgo criminal distinto al espacio nacional físico tradicional o, por el contrario, idéntico a este en sus caracteres esenciales.

- En segundo lugar, será necesario plantearse si **el cibercrimen es un delito nuevo o por el contrario es un delito viejo pero que sucede en un nuevo ámbito**. En este sentido, se plantean diferentes posturas. Desde una visión más extrema, la ciberdelincuencia es un tipo de delincuencia nueva para la cual no son válidas las teorías tradicionales creadas para explicar el espacio físico. En el polo opuesto, puede estar afirmando que el ciberdelito es idéntico estructuralmente al delito cometido en el espacio físico, cambiando únicamente el aspecto del mismo, pero en ningún caso sus caracteres configuradores. Y también cabe una posición intermedia, conforme a la cual la cibercriminalidad comparta con la delincuencia todos los elementos definitorios del concepto de "crimen", pero dándose los mismos de una forma tal en el nuevo ámbito que es el ciberespacio, que puede influir significativamente en la explicación del delito y, por tanto, en su prevención.

- En tercer lugar, también es importante plantearse cuál es **el rol que tienen los actores implicados en la producción del evento delictivo y si se**

puede incidir en ellos de manera específica para evitar la producción de los eventos delictivos.

- En cuarto y último lugar, será necesario, teniendo en cuenta las cuestiones anteriores, **estudiar si las teorías del crimen** concebidas **para el mundo físico se pueden trasladar al ciberespacio o si**, por el contrario, **será necesario hacer replanteamientos** de las teorías que se adapten a la realidad.

2. El ciberespacio como un nuevo ámbito de oportunidad criminal

La primera cuestión que debemos aclarar de cara a la prevención es en qué cambia el ciberespacio con respecto al espacio físico, es decir, cuáles son las singularidades que presenta, identificar los caracteres de su arquitectura, de su construcción como ámbito relacional, especialmente en lo que se diferencia de los del ámbito espacial o físico en el que tradicionalmente se han cometido las infracciones.

Antes de todo, es necesario explicar que el ciberespacio es el espacio virtual, no físico, determinado por la interconexión de personas a través de redes telemáticas, y dentro de él, uno de sus principales catalizadores es Internet, sistema global de información y comunicación basado en el protocolo TCP, que une ordenadores de todo el mundo y permite el acceso a cualquiera de ellos para obtener e intercambiar información de manera sencilla. Dentro de Internet, son muchos los servicios existentes, uno de los cuales es la World Wide Web, como conjunto de protocolos que permite acceder a información de forma remota, y que ha llegado a solapar como concepto al propio término de Internet, pese a que esta incluye otros servicios aparte de la WWW, como el correo electrónico, los canales IRC de conversación en línea, además de que son otras muchas las TIC que están integrándose hoy en Internet, como la telefonía electrónica o la televisión digital.

2.1. ¿Cómo es el ciberespacio?

El ciberespacio tiene como caracteres intrínsecos una concreta configuración de las coordenadas espacio/tiempo frente a la que tiene el que podríamos denominar espacio real o físico.

Decimos que el **ciberespacio** es un espacio porque en él las personas se encuentran y relacionan, pero mientras que el espacio físico existe antes y seguirá existiendo después de que termine la relación (cuanto menos mientras exista un observador), el ciberespacio agota su existencia en cuanto el mismo sirva para la comunicación entre los sujetos, dado que sin interacción no hay red.

Así, frente al espacio geotécnico como la tierra, que existe independientemente de los actos de la gente que tengan lugar en ella, y que solo puede ser ocupado a la vez por un mismo ente, el ciberespacio existe en cuanto en él se interacciona y es posible que sea ocupado por muchos entes al mismo tiempo. De hecho, se suele utilizar como sinónimo de *ciberespacio* el concepto de *espa-*

cio virtual, como antitético al espacio "real". La simultaneidad, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la de distancia. Evidentemente, el ciberespacio es real en el sentido de que existe, pero se trata de una "especie nueva" de espacio, invisible a nuestros directos sentidos y en el que las coordenadas espacio-tiempo adquieren otro significado y ven redefinidos su alcance y límites.

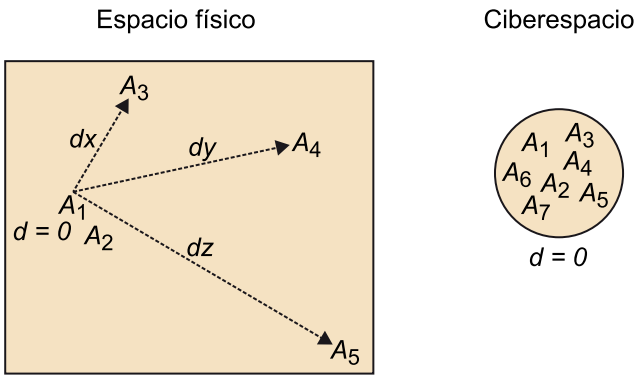
En realidad, pues, la idea de la "virtualidad" del ciberespacio deriva de la tradicional identificación entre espacio (físico) y distancia. En el ámbito de comunicación configurado por **Internet no hay distancias, pero sí espacio.** Así, el ciberespacio supone la contracción total del espacio (de las distancias) y a la vez, la dilatación de las posibilidades de encuentro y comunicación entre personas. Internet ha contraído el mundo acercando a un mismo lugar interactivo a personas que pueden estar en coordenadas espaciales separadas por miles de kilómetros. El espacio se contrae, la intercomunicación se expande, y ello influye evidentemente en la configuración social. Mientras que el espacio de las sociedades tradicionales estaba dominado por la contigüidad, por las relaciones de proximidad a nivel familiar, vecinal, local y supralocal, en la sociedad actual, las relaciones se canalizan a través de redes, lo cual favorece un desplazamiento de la información y de la comunicación mucho mayor. Es a través de redes, pues, como se crean las nuevas comunidades virtuales entre personas que pueden estar separadas por el espacio físico, pero a las que les unen los intereses e inquietudes y que, por ello, se configuran como comunidades con una lógica distinta a las de las tradicionales comunidades físicas.

El ciberespacio, en todo caso, convive con el espacio físico o terrestre, y también tiene, en algunos aspectos, una relación directa con él que no debe ser obviada: las redes telemáticas que conforman el ciberespacio vienen a unir, de forma virtual pero también física, terminales o sistemas informáticos que están ubicados en espacios terrestres concretos, en países nacionales determinados con contextos sociales de facilitación del acceso a Internet específicos, así como con regímenes jurídicos distintos, que pueden afectar, por ejemplo, a las obligaciones de los prestadores de servicios respecto a la identificación de los titulares de las direcciones IP. Además, también va cambiando la relación entre el espacio físico y el virtual: hace unas décadas era necesario un lugar físico fijo para entrar en el ciberespacio, mientras que hoy, gracias a las redes Wifi, y en particular a la nueva tecnología de la telefonía móvil, es posible conectarse desde prácticamente cualquier lugar físico del planeta y estando en movimiento.

Pero ese espacio geográfico en el que se encuentran las terminales es irrelevante para la comunicación entre personas en el ciberespacio. Lo realmente importante es que mientras que para la comunicación en el espacio físico era necesaria una cercanía (en términos de distancia) entre emisor y receptor, la

misma ya no es necesaria en el ciberespacio: ahora pueden hacerlo al mismo tiempo (o en tiempos separados, sobre lo que trataremos más adelante) y en el mismo (ciber)espacio, pero en distintos espacios geográficos (o a distancia).

Figura 1. Contracción de la distancia en el ciberespacio y expansión de la capacidad comunicativa



Abreviaturas: A_1 necesita $d = 0$ para comunicarse con A_2, A_3, A_4, etc.

La **distancia** deja de ser un obstáculo, por tanto, para la comunicación en el ciberespacio, de modo que esté donde esté el sujeto al que va dirigida la acción en Internet, el coste de realización es exactamente el mismo, dado que la distancia física no tiene relevancia en el ciberespacio.

Al afirmar que el ciberespacio es un "nuevo espacio", estamos anticipando la respuesta sobre la incidencia del ámbito en la otra dimensión, el tiempo. Internet también cambia el tiempo, su percepción social, así como la forma en la que el mismo tiempo se organiza.

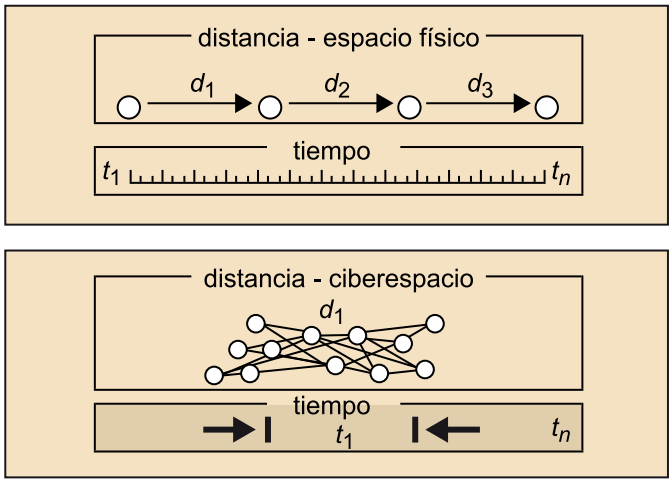
La **contracción del espacio** conlleva, en primer lugar, un aumento de la importancia del tiempo, y en segundo lugar, una compresión del tiempo necesario para la comunicación social. El tiempo necesario para la comunicación entre dos personas separadas por un espacio físico también se contrae ante la ausencia de la distancia y la aparición de un espacio virtual de intercomunicación inmediata. Así, lo que en el espacio físico nacional exige mucho tiempo, puede ser llevado a cabo de forma inmediata en el ciberespacio, con la consiguiente "aceleración de la vivencia subjetiva del tiempo", dado que en Internet los eventos suceden mucho más rápidamente que en la vida no virtual.

En todo caso, con el tiempo ocurre algo similar a lo que sucede con el espacio: la contracción en el sentido de reducción del tiempo necesario para llevar a cabo una determinada tarea conlleva un estiramiento de las relaciones sociales en cuanto que el avance de las tecnologías de la comunicación ha permitido salvar las "distancias temporales" entre las sociedades y acercarlas hasta convertir el contacto entre ellas en algo instantáneo. Como se ve en la figura 2, al

no requerirse en el ciberespacio recorrer una distancia para la comunicación, las posibilidades de contacto con múltiples sujetos aumentan y se reduce el tiempo necesario para ello.

En última instancia, puede decirse que Internet reduce los costes temporales exigidos en el espacio físico para cualquier tipo de comunicación entre personas.

Figura 2. Contracción del tiempo



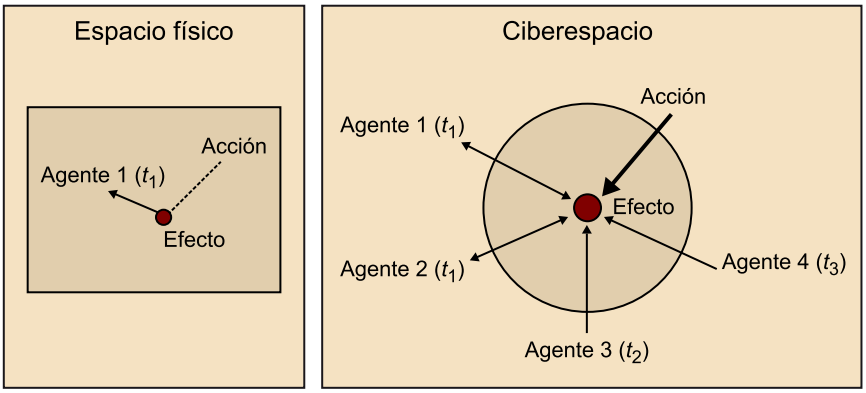
El tiempo necesario para la comunicación disminuye al no existir distancias en el ciberespacio

Y no es el único cambio que podríamos asignar al "tiempo" en el ciberespacio. La configuración comunicativa de este nuevo ámbito de intercomunicación social puede hacer que acciones cuyos efectos se produjeran de forma instantánea, pero caduca, tengan un funcionamiento temporal distinto: **que los efectos se produzcan instantáneamente pero sean perceptibles de forma perenne**.

Así, las conductas ejecutadas a través del ciberespacio, especialmente aquellas consistentes en la publicitación de contenidos, pueden quedar fijadas durante un tiempo indeterminado y seguir desplegando efectos aunque su ejecución solo haya durado un instante. La razón es la estructura comunicativa de Internet de constituir un espacio vasto que puede expandirse y contraerse, en el que las cosas pueden estar en un sitio y luego en otro, y en el que la comunicación entre personas en el ciberespacio puede producirse en tiempos distintos, en el sentido de que el emisor puede enviar un mensaje comunicativo en un momento temporal determinado y no ser recibido hasta mucho después por el receptor. Así, y como se trata de reflejar en la figura 3, mientras que en el espacio físico las acciones producen efectos en un determinado momento, en el ciberespacio el efecto puede quedar fijado durante un tiempo indeter-

minado y afectar a un agente determinado en el momento en que se realiza, pero también en un momento posterior cuando otro agente interaccione con dicho efecto.

Figura 3. Fijación de los efectos en el ciberespacio



La acción se ejecuta en cierto momento, pero A_3 y A_4 interaccionan con ella en momentos posteriores

Es cierto que en el espacio físico esto también es posible. Pero qué duda cabe de que el ciberespacio modifica la capacidad de control por parte del agente del hecho en relación con el elemento temporal. Y lo mismo sucede con el elemento espacial: en el espacio físico el agente tenía, cuanto menos generalmente, un mayor dominio sobre las coordenadas espacio-temporales del hecho, en el sentido de que podía definir el ámbito geográfico en el que iba a comenzar a producir efectos (aunque después estos pudieran escapar a lo deseado), así como el momento o instante temporal en el que iban a comenzar a hacerlo. También era posible, en muchos casos, definir concretamente el espacio físico en el que el hecho del agente iba a terminar de producir efectos, cuanto menos los más directamente derivados del mismo; y, de igual modo, el tiempo que iba a durar el hecho. **En el ciberespacio es más difícil concretar el ámbito geográfico-espacial en el que el hecho va a desarrollarse**: algunas acciones se pueden dirigir concretamente contra un usuario, un colectivo o una institución determinada, pero incluso en esos casos **la propagación de los efectos es más sencilla al no necesitar "recorrer distancias"**.

Otras acciones, además, son incontrolables en cuanto a su dimensión espacial: una vez se difunde un contenido en Internet o se propaga un *malware* a un colectivo indeterminado, es casi imposible saber quién, desde cualquier lado del mundo, se verá afectado por los mismos. Y si lo observamos desde la perspectiva contraria, la complejidad para la concreción de la causa a la que se puede atribuir el resultado o efecto es de similar entidad: mientras que la concreción del espacio geográfico donde se ha causado un determinado daño nos puede ayudar a identificar al responsable del mismo, en el ciberespacio la identificación geográfica y temporal de un efecto o consecuencia no nos asegura ningún tipo de cercanía espacial o de tiempo con la causa. No es que no haya transferencia, que la habrá, y por tanto huella, que será digital, sino

que **no habrá transferencia espacial**: la seguridad (o alta previsibilidad) de que el criminal deberá estar en un espacio determinado simplemente por el hecho de que el daño se haya producido en un lugar concreto.

Y lo mismo ocurrirá con el tiempo: que los efectos de una acción surjan en un determinado momento no asegura, en el ciberespacio, que el hecho se haya iniciado por parte del sujeto en ese instante temporal. Por el contrario, los agentes pasivos pueden convertirse en activos en el ciberespacio: es posible que un agente realice algo y "deje" el ciberespacio, y que sea otro sujeto el que interaccione con lo hecho por el primero posteriormente e independientemente de la voluntad del primero.

Lo relevante, en todo caso, es que en el ciberespacio las coordenadas espacio-temporales se ven significativamente modificadas: por una parte, se comprimen las distancias y el tiempo que cuesta recorrerlas; por otra, y derivado de lo anterior, se expanden las posibilidades comunicativas entre las personas y los efectos de los hechos que apenas se ven limitados espacial o temporalmente. Simbólicamente, acudiendo de nuevo a la geografía para explicar el efecto de todo esto, podríamos decir que el ciberespacio es un espacio mayor, más amplio, y también más duradero, de una percepción de los efectos más dilatada en el tiempo que el espacio físico. Lo que esto quiere decir es que cualquier agente en el ciberespacio, salvo el impedimento del contacto físico directo, tiene menos restricciones espaciales y temporales para sus actos que en el espacio físico. También, que los efectos de las conductas, las consecuencias plasmadas en unas coordenadas espacio-temporales determinadas, ofrecen menor información en el ciberespacio que las coordenadas espacio-temporales del acto al que se deben atribuir las mismas –y por ello, del agente causante– que en el espacio físico.

Por supuesto, todo esto va a influir en la configuración del (ciber)crimen, como evento social que es. Y si la criminología ha tratado desde siempre explicar este fenómeno –y especialmente en los últimos años, donde ha centrado su interés en el entorno en el que actúa, cuya arquitectura no es comparable al nuevo ámbito de intercomunicación social en el que también pueden producirse eventos criminales–, es evidente entonces la necesidad de replantear la vigencia de esas teoría para este nuevo tipo de delitos o, cuanto menos, adaptar sus desarrollos al nuevo espacio.

Antes de ello, sin embargo, conviene explicar otro tipo de caracteres que configuran también el ciberespacio y por ello, van a determinar cualquier fenómeno social que tenga lugar en él.

Uno de los caracteres básicos que acertadamente se suelen atribuir a Internet es el hecho de que el mismo esté **deslocalizado**. El ciberespacio, podríamos decir, no está situado en un sitio en concreto, sino que, en sentido funcional, está en todos a la vez pero en sentido físico, en ninguno. En realidad este no es ningún carácter extrínseco al fenómeno, sino algo intrínseco al ciberespacio: es su propia esencia como fenómeno (no) espacial, y que hemos analizado anteriormente.

No puede negarse, sin embargo, que tal carácter no tendría la importancia que tiene si no viniera unido a otro elemento que podríamos denominar accesorio, en cuanto que podría imaginarse un ciberespacio configurado sin él, pero esencial y definitorio de lo que para todo el mundo constituye en la actualidad ese nuevo ámbito social que es Internet: la transnacionalidad.

La **transnacionalidad** es la inexistencia de fronteras o distancias, ni aparentes ni reales, en un ámbito digital de interacción social que no pertenece a ningún Estado nacional concreto, pero que, a la vez, permite el acceso a sus servicios desde cualquiera de ellos.

La transnacionalidad del ciberespacio se traduce, a los efectos que nos interesan, en la total ausencia, para la comunicación e interacción entre individuos, de barreras que no sean impuestas o configuradas por el propio sujeto. Desde cualquier Estado nacional es posible acceder a cualquier Estado nacional, y un contenido vertido en una página web localizada en un servidor de un Estado concreto y colgada por un sujeto de un determinado Estado, puede ser vista por cientos de personas en cientos de sitios distintos en el mundo. Desde una perspectiva sociológica, es obvio que la transnacionalidad del ciberespacio lo configura como un ámbito de intercomunicación social nuevo que contrasta con las posibilidades de comunicación extranacional en el espacio físico. En el ciberespacio, la trasnacionalidad se mezcla con la localidad, en el sentido de que ya no es necesario, para tener un contacto o comunicación con un Estado, región o localidad, distinta a la propia, realizar un traslado físico, sino que puede accederse a lo trasnacional desde lo local, incluso desde lo personal o íntimo que, por tanto, puede quedar ya, tan solo dependiendo de la decisión del propio individuo, al acceso de muchas más personas de lo que era posible anteriormente. Aumentan por tanto, en el ciberespacio, las facilidades para la multicomunicación social (transnacional), y disminuyen así, los impedimentos para la comunicación entre personas, cuanto menos el que la misma se limitaba a las personas que se hallasen físicamente próximas. Lo mismo ocurre con los bienes: ya no es necesario, en el ciberespacio, un contacto físico entre agente y bien para que exista el acceso, y desde luego, no es necesario que se esté en el momento del intercambio o de la adquisición (lícita o ilícita) en el mismo lugar físico, sino que es posible que un sujeto desde un Estado nacional acceda a otro y acceda a un bien, digitalizado, pero con valor económico.

Otro carácter extrínseco de máxima importancia es la **neutralidad** en el ciberespacio, que implica la libertad del usuario a la hora de transitar por el mismo sin fronteras pero también sin censuras de acceso por parte de nadie. El carácter neutro de Internet deriva de la imposibilidad de bloquear conexiones entre nodos en la Red, lo que permite que una vez tengan acceso a Internet, ni siquiera el propio operador pueda impedir el acceso a una web o a un servicio elegido por el usuario.

Aunque se trata de un carácter extrínseco, dado que podrían establecerse restricciones por medio de una reconfiguración de Internet que permitiera, por ejemplo, bloquear la capacidad de un usuario para emitir información o para acceder a un sitio web, es consustancial al ciberespacio que conocemos, en el que no hay más restricciones que las que se imponga el usuario, su carácter neutro. Es obvio, precisamente por ello, que el control de informaciones y contenidos, por parte de quien quiera llevarlo a cabo, es complejo en el ciberespacio, aunque es discutible que lo sea más que en el espacio físico. La dificultad de controlar las comunicaciones entre usuarios particulares en el ámbito real puede ser incluso mayor al no quedar, como en el ciberespacio, constancia o huella de lo comunicado. Lo que sí es mayor, sin lugar a dudas, es la capacidad de la información para difundirse en un espacio universal y popularizado, y eso es lo que aumenta su importancia, también su valor, y en algunos casos su capacidad no puede negarse, para causar daño a bienes esenciales, lo cual puede servir de razón o de excusa para Estados o algunas organizaciones, para tratar de crear un ciberespacio distinto, con nodos conectados que en su parte central dependan de alguien y que, por ello, le permitan impedir el acceso a determinadas webs o la navegación a usuarios específicos.

En relación con la transnacionalidad y el carácter neutro de la Red, también podríamos citar como carácter extrínseco pero configurador del ciberespacio, su **descentralización** o, quizás mejor, su no centralización y concretamente su carácter **distribuido**, dado que en la estructuración de Internet no existen nodos centrales pero tampoco nodos que actúen como centros locales, sino que se trata de una malla y en la caída de un nodo no imposibilita que la información siga fluyendo.

Por otra parte, y relacionado con ello, **no existe en Internet autoridad centralizada alguna**, ni siquiera órganos o instituciones de control de la información circulante que puedan establecer algún tipo de censura sistemática o control de los contenidos. Internet no está sometida a las leyes nacionales de un único país, ni a unas normas propias aceptadas por todos los que la conforman, y esto conlleva que los controles gubernamentales resulten poco efectivos, al existir variadas formas de evitar los que van imponiendo los Estados nacionales. Es obvio, sin embargo, que la existencia de este espacio transnacional, neutro y distribuido, con las consecuencias que conlleva, produce una tensión, en este caso en el plano jurídico, con la casi contradictoria existencia

de Estados nacionales con legislaciones distintas reguladoras de este u otro fenómeno. Si bien no existe un control global de la Red, los gobiernos nacionales han comenzado a tratar de regular Internet ante el potencial riesgo que supone y su popularización en todas las escalas sociales. Pero en todo caso, la adopción de decisiones nacionales apenas soluciona el problema, como es obvio. El potencial riesgo que supone la transnacionalidad del cibercrimen y que le convierte en uno de los mayores desafíos planteados en la actualidad, deriva de **lo complejo que resulta responder localmente a riesgos globales**.

Desde la perspectiva criminológica que ahora nos interesa, podríamos afirmar que esto es conocido por los cibercriminales, en el sentido de que son conscientes de que pese a realizar conductas que en el Estado en el que producen efectos pueden resultar delictivas, el hecho de hacerlo desde un Estado distinto complicará enormemente la persecución penal por las mismas. Además, esta transnacionalidad y carácter distribuido del ciberespacio, unidos a la existencia de múltiples normas distintas en diferentes Estados, y a la característica que después analizaremos relativa a la permanente revolución tecnológica que se produce en este nuevo ámbito social, conlleva que, al contrario de lo que suele suceder en el espacio físico, no sea nada sencillo determinar para algunas conductas si las mismas son socialmente adecuadas o incluso legales o no lo son. El ciberespacio difumina la apariencia de legalidad de las conductas.

Otro carácter a destacar del ciberespacio como ámbito de riesgo consiste en su carácter **universal**, y no en este caso en el sentido de transnacional, sino en el de global, colectivo o popular. En el mundo podemos hablar de aproximadamente mil millones de usuarios y por tanto, de millones de objetivos sobre los que pueden actuar los criminales.

Popularización de la informática

En las últimas décadas se ha producido una popularización de la informática, un aumento de las facilidades para adquirir o acceder a terminales y muy especialmente, a la interconexión entre todas ellas en un espacio de comunicación global que también se ha generalizado. Además, y pese a que se creyó durante los primeros años que sería Internet de uso esencial para empresas e instituciones, la evolución de las tecnologías para el acceso a la Red ha hecho que hoy en día sean usuarios particulares los que principalmente usen Internet como vehículo de comunicación personal. El auge de las redes sociales y la mejora de la educación en el uso de las TIC desde la infancia, ha llevado a que los menores desde los nueve años, hasta los mayores de sesenta y cinco años, sean todos usuarios de una red que también en ese sentido es global.

La universalización de Internet también tiene que ver, además de con su bajo coste, con el **anonimato** que el mismo confiere. Pese a que desde algunos sectores se está intentando construir algún tipo de sistema que permita la identificación de los usuarios, parece difícil de imaginar un ciberespacio en el que todos o la mayoría de los que intervienen en él estén identificados. Aunque la determinación del sistema informático que navega por el ciberespacio no parezca tan compleja actualmente, sí lo es, por el contrario, la concreción del sujeto que ha utilizado el mismo para realizar la infracción, especialmente en la actualidad, donde existen múltiples cibercafés desde los que comunicarse en el ciberespacio, redes Wifi que permiten acceder desde sitios abiertos, etc.

A ello hay que sumar los proveedores de servicios gratuitos que no exigen la identificación de los usuarios, los múltiples sistemas que permiten enviar correos electrónicos de forma anónima y, ya más en el ámbito del evento criminal, las posibilidades actuales de infectar un determinado sistema informático para convertirlo en un robot (*bot* o *zombie*) y utilizarlo para realizar la actividad criminal, logrando que ni siquiera sea posible la identificación de la IP, desde la que, en realidad, se ha generado el ataque, así como otros factores relevantes, como la transnacionalidad y la diversidad de prestadores de servicios que operan en Estados con regímenes jurídicos distintos, que no siempre obligan a la identificación de las terminales en red. El anonimato tiene como consecuencia un aumento de la sensación de impunidad y esta, a su vez, un incremento del riesgo de que el agente acabe por ejecutar el delito.

Otra característica que hay que tener presente es que el ciberespacio está sujeto a una **evolución tecnológica permanente**. Las TIC se caracterizan por sufrir modificaciones importantes de forma casi constante, de forma tal que los modos de comunicación social, de intercambio económico, de difusión de contenidos, o cualesquiera otros que se utilizan en un determinado momento, pueden ser sustituidos en muy poco tiempo por evoluciones que pueden ir desde una pequeña modificación hasta una auténtica revolución del sistema. Así, la evolución de Internet parece imparable, tanto en la aparición de nuevos servicios, como en la mejora y modificación de las formas de acceso.

La importancia que esto tiene es más que evidente: por una parte, las barreras de protección del tipo que sean, para los intereses personales y sociales que parecen en un determinado momento eficaces, pueden dejar de serlo en muy poco tiempo, y bienes que parecen intocables frente a las TIC pueden pasar a ser susceptibles de ataque en un instante; por otra parte, el derecho camina totalmente "a remolque" de un contexto social que va cambiando, y las soluciones jurídicas de hoy parecen obsoletas y de ayer cuando entran en vigor.

Por otra parte, no hay que despreciar la importancia de que el ciberespacio esté sometido a cambios procedentes de los propios usuarios. Son los usuarios los que han hecho de Internet lo que es, y son ellos los que constantemente lo modifican y crean. Y esto se debe, no solo a que la interacción social con cualquier tecnología incida en su propia estructura, sino a que Internet es una tecnología muy flexible y dúctil que "permite el efecto de retroacción en tiempo real". Internet se está configurando como un espacio abierto en el que, al contrario que en otros sistemas, los cambios y modificaciones devienen de la propia intervención del conjunto de usuarios, y no de un ente central.

Esta relación directa entre el usuario e Internet, entre su configuración y uso con el agente, es más poderosa que en la realidad del espacio físico, debido probablemente a otros de los factores que hemos hablado antes como la des-

centralización y la popularización del medio. Lo importante, en todo caso, es el efecto que produce: el usuario se siente parte definitoria del ciberespacio y, por tanto, parte decisoria del mismo, especialmente en su configuración como espacio de libertad. En el espacio físico-geográfico, definido por unas fronteras y bajo la autoridad de un Estado concreto, el ciudadano tiene definidas muy estrictamente sus posibilidades democráticas: puede elegir a los representantes políticos o directamente a los gobernantes, puede proponer de forma más o menos directa la aprobación de normas jurídicas, etc.; y también puede configurar los usos sociales, si bien al estar ellos generalmente definidos con la evolución de la sociedad, resulta complicado para el ciudadano una influencia directa en ellos. En el ciberespacio es distinto.

En cuanto a la participación en procesos formales de decisión democrática, la misma no es posible en el ciberespacio y sin embargo, su democratización (o la apariencia de ella) es mucho mayor en cuanto que, al no existir autoridades y ser universal y popular, es el conjunto de los ciudadanos de Internet el que acaba decidiendo cuáles son las normas sociales básicas de funcionamiento interno. Es evidente que esto no es derecho en un sentido estricto, pero también lo es que son usos sociales que, en un ámbito como el de Internet donde son los intereses económicos y personales los que mandan, acaban convirtiéndose en reglas de conducta válidas para el funcionamiento de las relaciones en Internet. Además, y precisamente por ser un ámbito social nuevo, cambiar y definir las normas (llamémosle así) éticas del mismo es mucho más sencillo para el usuario, pues no hay usos sociales impuestos sino que se van creando con la interacción de todos los nuevos.

Las consecuencias de esto para el entorno social del ciberespacio, a los efectos que nos interesan, son variadas, pero destaca el hecho de que en el mismo no está tan definida la ética o moral imperante como en el espacio físico sujeto a una soberanía nacional, básicamente porque los propios usuarios, con sus conductas, la pueden cambiar. Es posible, y de hecho es lo que está sucediendo con instituciones como la propiedad intelectual, pero no solo con ella, que las reglas que rijan para el espacio físico se consideren, por parte de los usuarios, no aptas para ese nuevo ámbito que ellos acaban definiendo con su actuar. Esto no significa que el derecho deje de regir, pero sí que su capacidad de influencia reguladora puede disminuir, en cuanto que, a mayor correspondencia entre lo normado y lo aceptado socialmente, mayor cumplimiento de las normas.

Es obvio que todos estos factores, intrínsecos y extrínsecos, de ese nuevo ámbito que es el ciberespacio van a determinar todos los fenómenos que en él se produzcan, entre ellos el que nos ocupa, el crimen.

2.2. La oportunidad delictiva

Las primeras aproximaciones de la criminología al fenómeno del cibercrimen se centraron en la discusión acerca de las motivaciones del *hacker*, quizás porque en aquellos momentos la criminología se centraba en el estudio del sujeto

criminal, en la comprensión de los condicionantes de su conducta y sus modalidades. En los últimos años se han sucedido diferentes estudios que han tratado de comprender el fenómeno de la criminalidad aplicando teorías de la oportunidad como la teoría del autocontrol, la teoría de la decisión racional, la teoría del aprendizaje social, la teoría del control social, la teoría del etiquetamiento o de las actividades cotidianas.

Si tomamos en consideración que la teoría de las actividades cotidianas, como parte del germen de todas las actuales teorías de la oportunidad o del día a día –que en los últimos años parecen estar en el centro de los principales debates criminológicos superando las expectativas que se marcaban para la criminología ambiental y que han dado lugar, en conjunción con la teoría de la decisión racional, a los desarrollos sobre la prevención situacional del delito–, partió, como una de sus premisas fundamentales, de la idea de que la modernidad, y en ella la evolución tecnológica, llevaba implícita el aumento del contacto entre potenciales autores, potenciales víctimas y, en algunos casos, la disminución de guardianes capaces de evitar el crimen, con el consiguiente aumento en las tasas de criminalidad.

Lo cierto es que si en el momento en que se enunció esta teoría, ello se apoyaba en evoluciones tecnológicas, como el automóvil, y sociales, como la igualdad entre hombre y mujer, que habían modificado la relación entre el ofensor motivado, el objetivo y la ausencia de mecanismos de defensa; hoy, la aparición de un nuevo espacio de comunicación personal transnacional, universal y sujeto a revolución permanente, como es el ciberespacio, anticipa, si no un aumento de la criminalidad –lo cual tendrá que evaluarse a más largo plazo–, sí, por lo menos, la existencia de un nuevo contexto de oportunidad criminal que coexistirá en el tiempo con el de la realidad física, y que pudiendo compartir con este el que el delito dependerá de la relación entre victimario, víctima y mecanismos de protección, divergirá en la manifestación concreta de estos mismos factores, fruto de la especialidad del medio en que convergen.

En todo caso, lo que hace especialmente apta la teoría de las actividades cotidianas es el hecho de que esta pone el foco de análisis del evento criminal, ya no tanto en el agresor o criminal, como en el propio espacio y en cómo el mismo puede incidir en la aparición del delito. El nacimiento de un nuevo ámbito de comisión delictiva, como el ciberespacio con caracteres intrínsecos y extrínsecos significativamente distintos al espacio físico donde se siguen cometiendo el mayor número de delitos, conlleva que sea oportuno partir de aquellas teorías que prestan atención al lugar de comisión delictiva para comprobar los nuevos caracteres del evento criminal en el ciberespacio.

Y hay un último punto de unión entre el enfoque de la oportunidad y el cibercrimen, que tiene que ver con la necesidad de acudir para la prevención de esta nueva forma de delincuencia a aquellas teorías que pongan el mayor foco posible en el control no formal, debido a la probada ineficiencia del control formal, y especialmente, de las normas jurídicas nacionales frente a este tipo de crimen. En efecto, dan de alguna forma por sentado que el sistema de la justicia penal tiene una capacidad limitada para lograr efectos preventivos, por lo que centran su atención en el mundo de cada día para intentar actuar en él y prevenir así el delito. Es obvio que este enfoque tiene especial sentido ante un tipo de criminalidad como el que nos ocupa, que, debido a que se realiza en el ciberespacio transnacional y a su anonimidad –contra lo que, de algún modo, van a chocar la Administración de Justicia y el sistema penal nacional en general–, requiere poner el foco de atención para su prevención no solo en lo normativo y lo formal, sino, más allá de ello, en lo ambiental y en el propio actuar cotidiano de quienes acceden e interactúan en Internet.

Todo lo anterior no supone, por supuesto, ni la consideración de que el enfoque de la oportunidad sea más válido como pensamiento criminológico que el de las tradicionales teorías criminológicas o del delincuente, con el consiguiente rechazo de las múltiples críticas dirigidas al *opportunity approach*, ni que sea el único posible para la cibercriminalidad. Simplemente sirve para explicar la decisión tomada de utilizar este enfoque para comprobar la importancia del cambio del entorno espacio/temporal en el fenómeno criminal y así, analizar el evento cibercrimen. Es evidente la potencial capacidad de algunas de las tradicionales teorías de la criminalidad o del delincuente para la explicación de muchas modalidades de cibercriminalidad, así como que esta visión es perfectamente compatible con una intervención en el ámbito de la oportunidad, pero también lo es que aquellas teorías que ponen más énfasis en la relación de lo ambiental o espacial con la propia motivación del criminal reflejarán mejor los cambios que puede suponer para el crimen como evento el que el lugar de realización sea el ciberespacio.

Prevención del delito

"La prevención del delito es una responsabilidad de todos y no solamente de las agencias de control social formal o el sistema de justicia penal."

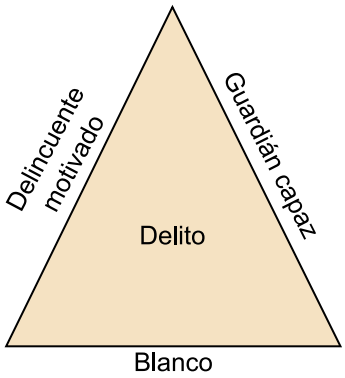
J. J. Medina Ariza (1998, pág. 281)

2.3. Teoría de las actividades cotidianas en el ciberespacio

La teoría de las actividades cotidianas de Cohen y Felson (1979) afirma que el delito se produce en un tiempo y un lugar, pero no exige que sea físico, aunque implícitamente lo estuviera presuponiendo. Por supuesto, el lugar de comisión de un crimen puede ser el ciberespacio que, como hemos visto, difiere en su arquitectura del espacio físico en el que solo podían cometerse los delitos hasta hace unas décadas.

Si en el ciberespacio puede cometerse un delito, en él tendrán que darse también los caracteres que se asignan al mismo. Es decir, si el crimen, como evento, depende de la presencia de un delincuente capacitado y motivado para el delito, un objetivo o víctima adecuada y la ausencia de un guardián capaz, en la primera fórmula de la teoría de las actividades cotidianas, así como de los demás elementos incorporados en las siguientes fórmulas, lo mismo deberá poder decirse del cibercrimen. Eso sí, al cambiar la configuración espacio-temporal del ciberespacio, el modo en que confluirán tales elementos hará que se relacionen entre sí y conformarán la ecuación del delito, será distinto. El triángulo del crimen seguirá teniendo los mismos elementos, aunque quizás los "ángulos", valga la expresión, sean distintos. O en otras palabras, el lugar "ciberespacio" no alterará los factores del crimen, pero sí la concreta expresión de los mismos y, por tanto, de múltiples elementos que debieran ser tomados en consideración en aras a la prevención del delito.

Figura 4. Triángulo del crimen



Para analizar las razones de los diferentes ángulos que conforman la interacción del agresor motivado con el objetivo adecuado en el lugar ciberespacio, hay que contrastar tales elementos con los caracteres intrínsecos y extrínsecos del ciberespacio, definiendo así los rasgos más singulares de ese nuevo ámbito de oportunidad delictiva y en comparación con el otro ámbito de oportunidad criminal, el del espacio real. El resultado de tal comparación, deberá servirnos para comprender las peculiaridades del cibercrimen, que deben ser tomadas en consideración para definir los instrumentos de prevención del mismo.

Por otra parte, y pese a que todos los elementos del evento criminal se explican al venir unidos entre sí, a efectos didácticos vamos a analizar el mismo estudiando de forma separada la incidencia del ciberespacio en cada uno de los elementos que conforman el triángulo del delito (tal y como quedaría con la primera configuración de Cohen y Felson), añadiendo a los gestores del lugar que se incorporan en el segundo triángulo y eliminando, por motivos obvios, el lugar (que es el propio ciberespacio).

2.3.1. El delincuente motivado

El agresor en el ciberespacio sigue motivándose sobre un determinado objetivo y en un lugar. Pero el campo de oportunidad de un agresor motivado (en abstracto) es muy amplio en el ciberespacio debido a la inexistencia de la distancia física como barrera o, dicho de otra forma, a la no necesidad de cercanía entre agresor y víctima para la (ciber)delincuencia, tal y como sí se requería generalmente en el espacio físico. Mientras que lo usual en la criminalidad suele ser que el delincuente realice el delito cerca de su propia residencia o cuanto menos que no se desplace a largas distancias, salvo en el caso de que el incentivo derivado del ataque al objetivo adecuado sea especialmente valioso, en la cibercriminalidad no hace falta salir de casa para atacar a bienes jurídicos que se encuentran físicamente muy lejos.

TIC y delincuencia

Es cierto que ya existían tecnologías que posibilitaban que el ataque criminal se realizara desde un lugar y los efectos se produjeran a miles de kilómetros de distancia. Pero también es claro que han sido las TIC las que han creado el ciberespacio, en el que la distancia física deja de ser una barrera infranqueable para muchos delitos, constituyéndose como un ámbito de oportunidad más amplio (siempre en términos potenciales): aumenta considerablemente el número de personas que pueden contactar unas con otras como agresores y objetivos adecuados, expandiéndose, por tanto, el ámbito potencial de oportunidad criminal.

Lo más relevante de lo señalado, en todo caso, y desde la perspectiva del agresor motivado, es que la compresión del espacio que supone el ciberespacio incrementa las "posibilidades de motivación" de un potencial agresor motivado. Lo hace al menos por dos razones:

1) La primera porque incrementa los objetivos potenciales sobre los que puede tomar la decisión de cuál es el adecuado, sin que la distancia ni el tiempo sean un elemento esencial de la decisión.

2) La segunda porque reduce el coste espacio-temporal que supone prácticamente siempre cometer un delito, tanto en términos de llegar al objetivo como en el de asegurarse la huida una vez el delito se ha cometido.

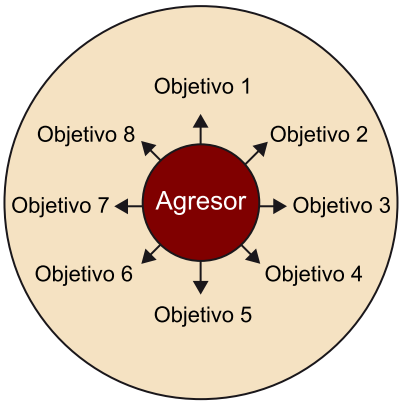
El que no exista un desplazamiento espacial y que el sujeto pueda "ahorrarse" tal coste, no significa que no haya un coste temporal para la realización de un ataque en el ciberespacio. Siempre lo habrá, y será mayor o menor dependiendo del tipo de cibercrimen. En el caso de los económicos, en particular el desarrollo de programas y técnicas o la propia búsqueda de vulnerabilidades, exigen a los *hackers* mucho tiempo, al igual que para el ladrón se exige preparación en el espacio físico.

En realidad, es este tiempo, el de preparación del ataque y de selección de los objetivos, el que se convertirá en el auténtico protagonista, en términos de coste, del ataque en el ciberespacio. De hecho, la selección de objetivos es la clave, como se ha visto, de gran parte de la cibercriminalidad económica, especialmente del *phishing*, tanto por medio de la búsqueda de vulnerabilidades en los sistemas para ser infectados como *bots*, como de la búsqueda de destinatarios finales a los que defraudar. Eso sí, se trata de un proceso de selección, y sobre ello se volverá más adelante, en el que interviene mucho la víctima, pues lo que hará el ciberagresor en muchas ocasiones es crear el software y el lugar en el que lo deja, y será la víctima con cierta vulnerabilidad la que, al interaccionar, será infectada y "atacada". En todo caso, costes temporales relacionados con la preparación y ejecución del crimen los hay tanto en el ciber como en el *offline*.

En lo que sí variará es en los **costes de desplazamiento y de huida** que están presentes en el crimen en el espacio físico, pero **no en el cibercrimen**. Así, mientras que el criminal en el espacio físico tiene que tener en cuenta el coste, en términos de distancia y tiempo, de la huida del lugar desde el que ha cometido el delito a un lugar seguro (como tiene que tener en cuenta la distancia y tiempo desde su lugar de origen a aquel en el que comete la infracción), el cibercriminal "se ahorra" estos costes.

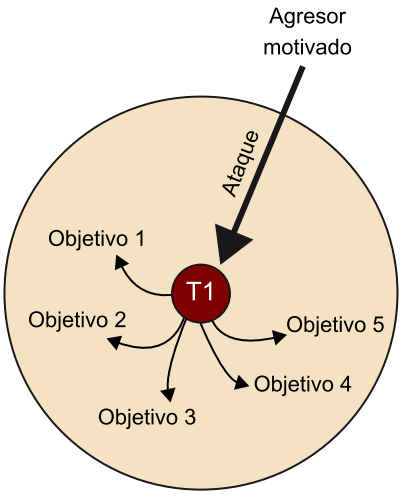
También en relación con el agresor y la incidencia en él de la arquitectura del nuevo ámbito en el que actúa, que es el ciberespacio, hay que señalar que las TIC pueden actuar como un "multiplicador de fuerza" que hace que personas con mínimos recursos puedan generar grandes daños para múltiples personas y bienes en el ciberespacio. Además, la expansión del ámbito comunicativo al que puede acceder un agresor motivado que supone el ciberespacio conlleva una multiplicación de la potencialidad lesiva de una conducta por comparación con lo que ocurre en el espacio físico. Es decir, aunque hay armas sofisticadas que permiten causar daños a múltiples bienes en el espacio físico y real, lo general es que la producción de daños a bienes existentes en lugares distintos (y desde luego en países distintos sería también válido como excepción para las armas), requiera de un tránsito del cibercriminal de un lugar a otro, que en el ciberespacio no es necesario. Esto ya ocurría con los delitos “de palabra” en relación con la televisión y otros medios de comunicación. En el ciberespacio aún es más significativo: como se ve en la siguiente figura, el agresor puede no solo seleccionar entre muchísimas víctimas potenciales sino que puede atacar a varias de ellas en el mismo instante y desde el mismo espacio, aunque ellas se encuentren en lugares situados a miles de kilómetros de distancia entre sí; e incluso aunque los efectos de los ataques no se desplieguen (o sí) en el mismo momento.

Figura 5. Multiplicidad de objetivos para un mismo atacante: un agresor actúa a la vez sobre varios objetivos



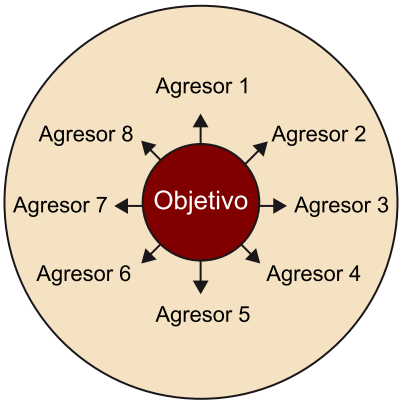
Además, el ciberespacio no solo permite al agresor motivado seleccionar entre varias víctimas el objetivo de su ataque, sino que la contracción de las distancias le ofrece la posibilidad de atacar a varias con una única conducta. Esto también es posible en el caso de la criminalidad llevada a cabo en el espacio físico-real, si bien las facilidades para ello en el ciberespacio son mucho mayores, especialmente en el caso de la modalidad de cibercrímenes, en los que la ilicitud deviene del contenido y en los que la mera publicitación de una página web con contenido nocivo o prohibido (ciberterrorismo, *hatespeech*, pornografía infantil, piratería intelectual, etc.) ya supone la afectación de múltiples bienes jurídicos o del mismo bien supraindividual pero con una mayor dimensión en la lesión.

Figura 6. Ataque múltiple: con la misma acción se atacan diversos objetivos (y en el mismo tiempo)



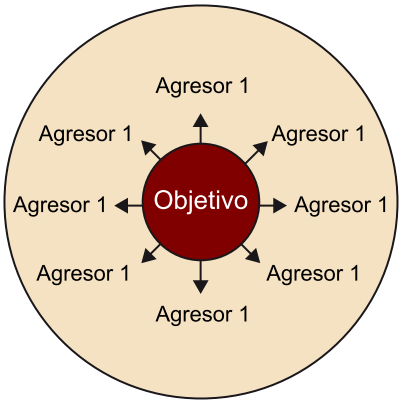
También es perfectamente posible en el ciberespacio que una misma víctima sea atacada de forma simultánea, y en el mismo espacio que ocupa, por múltiples agresores distintos. En este caso, el ataque se produce en el mismo (ciber)espacio, pero desde espacios (físicos) distintos y en momentos temporales que pueden ser idénticos en cuanto al despliegue de efectos pero no tienen por qué serlo en cuanto al momento de ataque.

Figura 7. Multiplicidad de atacantes para un mismo objetivo



Por último, el agresor puede utilizar uno o múltiples sistemas informáticos situados también en múltiples lugares (infecciones de *bot*) desde los que realizar ataques que pueden ocurrir de forma simultánea o secuencial y contra un único objetivo o contra objetivos que pueden ser múltiples e incluso indeterminados, sin que sea necesario para ello hacer ningún esfuerzo de traslado.

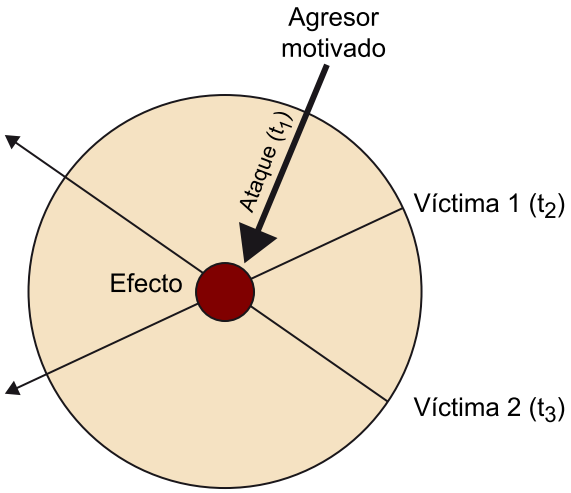
Figura 8. Multiplicidad de lugares en el ciberespacio que utiliza el agresor para atacar a la víctima desde un único punto en el espacio físico



Y todo eso, por supuesto, ejecutado por el agresor desde y sobre cualquier parte del mundo. Al fin y al cabo, la compresión o contracción de las distancias y la consiguiente expansión comunicativa en el ciberespacio no sería tan relevante si el mismo no fuera transnacional y se hubiera popularizado de la forma que lo ha hecho. En el ciberespacio, los ofensores con inclinaciones criminales pueden serlo de y desde cualquier Estado nacional y pueden actuar sobre víctimas de (y hacia) otros distintos, reduciéndose las barreras que el espacio suele imponer para ello. Pero además, al aumentar la cantidad de personas que utilizan Internet, también lo hace el número de potenciales delincuentes, y al unir el ciberespacio a miles de millones de ciudadanos en un "lugar común" en el que hay relaciones comerciales y personales, aumentan también los "objetivos adecuados" y, por tanto, las posibilidades de contacto entre unos y otros con el consiguiente potencial aumento de la criminalidad. En este sentido, el ciberespacio es, desde una perspectiva cuantitativa, un espacio de riesgo criminal con un “potencial” efecto multiplicador sin precedentes en la historia.

Además, y como se ha avanzado, la reducción de la distancia conlleva una reducción del tiempo como coste. Todos los ataques a uno o varios objetivos pueden realizarse en el mismo momento, sin que sea necesario el tiempo requerido para transitar la distancia que separa a los objetivos para que todos se vean afectados. Además, y siguiendo en el análisis de la incidencia de las nuevas condiciones ambientales en el factor "agresor motivado", pero prestando ahora atención al factor temporal, las especiales características del ciberespacio y de determinados instrumentos de comisión de los ciberataques, como los virus, permiten que en determinadas condiciones la presencia del agresor motivado tenga lugar en un momento de tiempo anterior al perfeccionamiento del ataque. Propiamente, el agresor motivado no desaparece, sino que simplemente su ataque se produce en un ámbito (y en un momento temporal) en el que la concreción del mismo ya no dependerá tanto de la propia conducta de este como de la de la víctima. Esto ocurre especialmente en el caso de los virus que son descargados en una determinada página web bajo la falsa apariencia de archivos de música o vídeo. El agresor motivado realiza su ataque dejando en el ciberespacio el instrumento del mismo como algo estático que espera a la conducta de la víctima para que el ataque termine perfeccionándose. Pero esto no significa que no haya agresor, sino que el mismo puede actuar multiplicando su capacidad lesiva en Internet sin las tradicionales limitaciones temporales y espaciales definidas por el espacio físico. Lo hará, eso sí, siempre que la víctima interaccione o, mejor dicho, con la víctima que interaccione con el efecto por él diseminado.

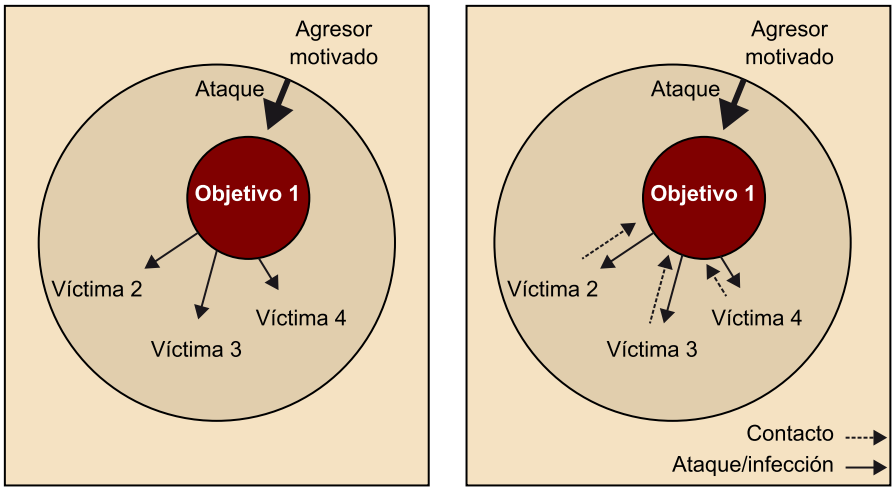
Figura 9. Fijación del ataque e interacción de la víctima: el ataque deja un efecto fijo en el ciberespacio, siendo la víctima la que interacciona con él



Y es que la contracción del espacio también puede tener importantes consecuencias en relación con los efectos del delito, muy en especial con alguno de los tipos de criminalidad en el ciberespacio caracterizada por la dinámica consistente en que la víctima-receptora del mismo se convierte, inmediatamente y sin quererlo, en emisor de un nuevo ataque en una cadena sucesiva que ni siquiera es controlada por el propio autor del crimen. Esto ocurre con la transmisión de virus, también con el envío de *spam*, e incluso, aunque de forma diferente, dado que en este caso es el receptor del mensaje el que tiene que

acceder a la comunicación, con la transmisión de contenidos ilícitos o nocivos (pornografía infantil, obras protegidas, *hatespeech*, etc.) en páginas web. Si los contenidos o los mensajes se transmitieran de forma física, la distancia entre emisor y receptor complicaría la multidifusión del ilícito. En el ciberespacio es distinto, pues la contracción del espacio y la interconexión de todos los sistemas hacen que la multiplicación de los efectos de la conducta sea prácticamente inmediata. En la criminalidad realizada en el espacio físico-real, es difícil encontrar algo semejante, a menos que se trate de la contaminación alimentaria o algunas formas de delincuencia ambiental, excepciones a la regla de que el delito produce sus efectos dañosos de forma controlada y dependiente esencialmente del actuar del criminal.

Figura 10. La víctima como instrumento de difusión del ataque



Por último, se ha relacionado acertadamente el aumento del riesgo criminal derivado de la potenciación del factor "agresor motivado", con el **anonimato** en Internet, que otorga una sensación de seguridad al infractor al ofrecerle un refugio aparentemente seguro en el que ocultarse, lo cual, a su vez, le permite reinventarse y adoptar nuevos personajes virtuales con los que, quizás, cometer delitos. Con el anonimato ocurre, por tanto, algo muy similar a lo que relatábamos en relación con la transnacionalidad, que incide en la desaparición del temor a ser identificado y en la consiguiente minimización del temor a ser detenido, frenos de la motivación criminal que le convierten en un *motivated offender*.

Desde la perspectiva de la teoría de la decisión racional, por tanto, el ciberdelincuente, incluiría dentro de los riesgos potenciales que tiene que sopesar frente a los beneficios de su agresión, la enorme dificultad que plantea hoy en día la identificación, en términos judiciales probatorios, del cibercriminal. Porque no solo se trata de la identificación de la dirección IP, sino de la posterior concreción del usuario concreto del sistema informático al que se ha concedido la misma. Es obvio que existen medios para evitar estos riesgos. Así, los mecanismos electrónicos de identificación, como el ID de usuario, sistemas automatizados de control del acceso o cámaras de vigilancia, pueden servir como elementos de disuasión al aumentar el riesgo percibido de ser detenidos.

Anonimato

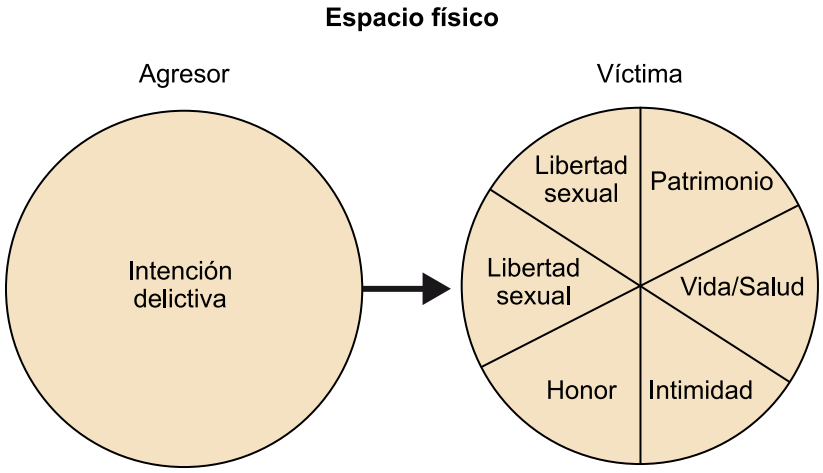
De momento, sin embargo, ello no parece posible, pues el anonimato no solo sirve a propósitos criminales, sino también a otros lícitos relacionados con la sencillez de la accesibilidad al ciberespacio, que difícilmente sería compatible con otros sistemas de identificación, que además podrían ser sencillamente falseados.

2.3.2. El objetivo adecuado

Lo que se ha afirmado hasta el momento del agresor motivado tiene consecuencias directas en el elemento "objetivo adecuado": el crecimiento del ámbito de riesgo no es solo por el agresor, sino por las víctimas potenciales, que también son muchas más al no ser necesaria una inmediatez temporal y una cercanía física entre agresor y objetivo. Del mismo modo, las dinámicas de los ciberataques y la potenciación de las facilidades para la agresión que conlleva el ciberespacio inciden en el objetivo adecuado de la misma, y lo mismo puede decirse de los efectos del ciberdelito. Al fin y al cabo, ya se ha dicho que la separación entre agresor motivado y objetivo adecuado tan solo es figurativa: **no hay motivación sin objetivo, y viceversa**.

En todo caso, debe precisarse lo que supone el incremento potencial de las posibilidades de contacto entre agresor y víctima en el ciberespacio. El contacto entre objetivo y agresor en el espacio físico es, generalmente, un contacto físico directo e inmediato, en el que todos los bienes personales de la víctima y los patrimoniales que lleve con ella, están expuestos y se convierten en potenciales objetivos adecuados para el ataque del agresor. Es cierto que la víctima potencial puede determinar en gran parte aquello que puede convertirse en objetivo adecuado, seleccionando los bienes con valor económico que lleva consigo, etc.; pero no puede eliminar del ámbito de contacto con las personas, otros bienes personalísimos que van indisolublemente unidos a ella. Prácticamente todo lo que ella es como persona, todo lo que forma parte de ella, se pone en contacto con el agresor en el espacio físico.

Figura 11. Contacto en el espacio físico



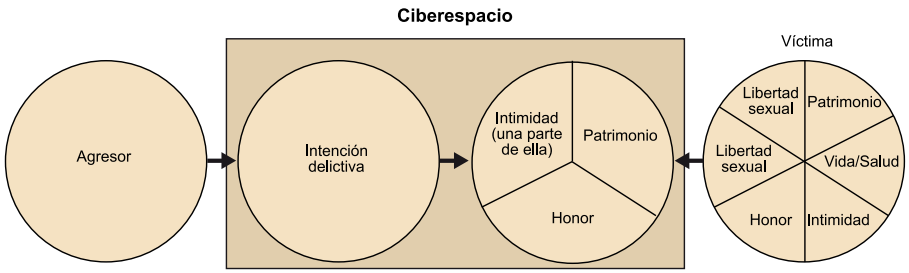
En el espacio virtual o ciberespacio, el contacto entre personas es distinto: no es la persona física la que se comunica directamente en un contexto espacio-temporal determinado con otra persona, sino una representación de la misma, en lo más esencial por ella definida, la que contacta en ese ámbito comunicativo que es Internet. La persona no entra con todos sus bienes y valores en el ciberespacio, sino básicamente con aquellos que ella elige de entre los que puede hacerlo. Al fin y al cabo, el primer límite que tiene la víctima para comunicarse con otra o para contactar en el ciberespacio es que no puede poner a disposición de otros su entidad física, de modo que los ataques a la persona que se dirijan directamente contra bienes, como la vida o la salud, no podrán ser llevados a cabo en Internet.

Además, y pese a que la persona puede ver atacados algunos bienes personalísimos, aunque ella no quiera ponerlos a disposición de terceros en el ciberespacio, en otros bienes, como los relacionados con la privacidad o el propio patrimonio, es la víctima la que decide, al incluir información personal en el ciberespacio o compartirla con otros, realizar actividades económicas, y además, situar tales bienes en ese ámbito de riesgo nuevo.

Bienes a disposición de terceros

Como ocurre con la libre formación de la sexualidad de los menores, que puede ser atacada al recibir una imagen de contenido sexual o similar.

Figura 12. Contacto en el ciberespacio



Los usuarios del ciberespacio pueden, por tanto, eliminar del ámbito de ataque aquellos bienes que no incorporen al ciberespacio. El crimen, por tanto, en cuanto al objetivo concreto sobre el que se dirige, puede ser evitado por la propia víctima en el ciberespacio desde el momento en que no es situado el mismo en el espacio virtual. Independientemente de su valor, si la víctima

no se incorpora al ciberespacio, el objetivo no existe y, por el contrario, la introducción de elementos en Internet conlleva inmediatamente el riesgo de que puedan ser victimizados. En este sentido, existen estudios empíricos que demuestran que prácticamente todas las modalidades de ataque se configuran en torno a una similar dinámica en la que el paso inicial suele ser el previo envío (la introducción), por parte de la víctima, de información personal a personas desconocidas. Ahora bien, y como se profundizará después, la mera introducción del objeto no es *per se* peligrosa, sino que constituye un primer paso que, si se une a la interacción de la víctima en el ciberespacio, ya puede conllevar riesgo de victimización.

Objetivo involuntario

La introducción de un objetivo en el ciberespacio, sin embargo, no siempre es voluntaria. En ocasiones, se trata de un proceso casi fortuito: el mero hecho de disponer de un sistema informático y de utilizarlo, conlleva la introducción de elementos relacionados con la privacidad, que sin quererlo pueden conllevar afectaciones a la intimidad o al propio patrimonio. La respuesta a un correo electrónico con el número de una cuenta bancaria supone la introducción del patrimonio disponible en esa cuenta, en el ciberespacio; y del mismo modo el acto de compartir una foto familiar en Facebook o información sobre un viaje reciente, conlleva el riesgo de que esto sea utilizado en contra de la dignidad o la intimidad de la persona.

En todo caso, el primer condicionante para que un objetivo sea adecuado a los efectos de la fórmula del cibercrimen es su introducción en el ciberespacio. A partir de que un objetivo se introduce en el ciberespacio, voluntaria o involuntariamente, el mismo puede convertirse en adecuado dependiendo de su valoración por parte del agresor motivado. Encontramos aquí, pues, la primera divergencia de las condiciones que hacen adecuado un objetivo para el cibercrimen, con las que, con el acrónimo **VIVA**, Felson definió como condiciones o criterios que reflejan la adecuación del objetivo para el delito:

- el **valor del objetivo** del crimen,
- su **inercia**,
- la **visibilidad física** del mismo y
- su **accesibilidad**.

La diferencia estriba en que previamente a todo ello, la introducción del objeto por parte de la propia víctima en el ciberespacio es condición primera y principal para su adecuación al cibercrimen.

Ahora bien, ¿y los demás caracteres del acrónimo VIVA? ¿Son válidos para el cibercrimen? Pues bien, el primer elemento que hay que analizar es el del valor del objetivo.

Independientemente del tipo de objetivo de que se trate (patrimonial, intimidad, libertad sexual, etc.), en el ciberespacio se da la particularidad de que cosas con poco valor intrínseco pueden adquirir un valor muy importante gracias a la facilidad para obtener información, relacionarla con la obtenida y convertirla en un objeto de riesgo.

Así, cuatro dígitos parecen no ser valiosos, pero si a ellos, por medio del *data mining*, se asocia el concepto "pin", y se relaciona con un determinado usuario, y si después se hace lo mismo con los números de una cuenta bancaria, etc., finalmente, tales números acaban por tener mucho valor. En todo caso, es evidente que a mayor valor del objetivo, mayor es la posibilidad de ataque, y esto será igual en el ciberespacio: los números de 20 dígitos son más buscados que los de 40, y las empresas más valiosas serán más buscadas por sus secretos comerciales que las no conocidas, por poner un ejemplo, y el cibercriminal decidirá según el valor que él mismo otorgue al objetivo.

Es más discutible, por el contrario, que sean válidos para la fórmula de la adecuación de los objetivos en el ciberespacio los restantes elementos del acrónimo VIVA. Comenzando por la inercia, Felson la definía como las propiedades intrínsecas de los objetivos que pueden hacer que la misma ofrezca distinto grado de resistencia al ataque.

Sin entrar en la discusión sobre la difícil separación entre inercia y accesibilidad, lo cierto es que en el ciberespacio los objetivos ofrecerán generalmente poca resistencia, dado que se trata de bienes informacionales que pueden ser descargados fácilmente sin resistencia alguna.

Los bienes en el ciberespacio apenas se diferenciarán entre sí por sus mayores o menores condiciones intrínsecas (y no relacionadas con los guardianes, pues esto es tema distinto), esto es, por la denominada inercia, para ser adecuados a recibir un ataque.

Algo similar ocurre con la accesibilidad, definida por Felson como la habilidad de un agresor para contactar con un objetivo y llevárselo de la escena del crimen.

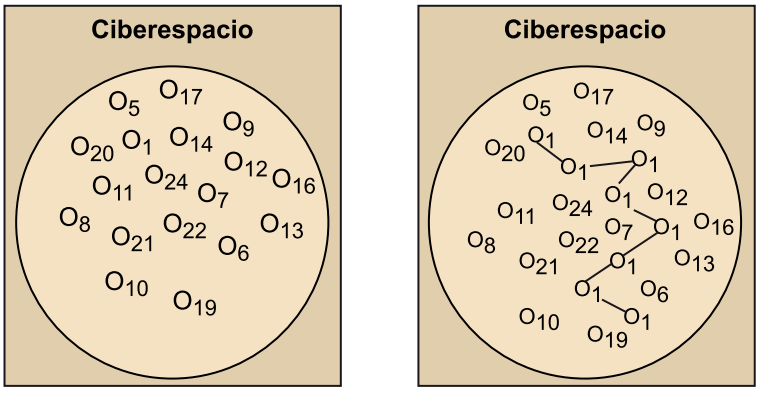
Como se puede comprender, dada la contracción de la distancia en el ciberespacio, todos los objetivos que entren en el ciberespacio son, en ese sentido, accesibles.

Puede haber observación del delincuente por medio de sistemas de rastreo o de señalización, pero eso no convierte al objetivo en menos adecuado, sino al gestor del lugar en más eficaz (o al guardián si deviene de la propia víctima el sistema e impide el ataque). Si a ello unimos que, en realidad, esta característica

está más asociada al agresor que a las particularidades del objetivo, podemos afirmar que la misma no es condicionante de la adecuación de un objeto en el cibercrimen.

Cuestión similar, pero no idéntica, sucede con la que Felson denomina visibilidad del objetivo, dado que si algo no es percibido por el agresor, no puede ser blanco suyo. El ciberespacio es tan ingente y tan universal, que es difícil hacerse visible, hasta el punto de que todos los usuarios conforman una maraña en la que es difícil distinguir a unos y otros. Lo que hace visibles a los sujetos en el ciberespacio es su interacción con otros sujetos y con otros servicios. A mayor interacción con otros agentes, con diferentes páginas web, con variados servicios, mayor posibilidad de ser percibido (ser visible) por parte de otros.

Figura 13. Visualización de objetivos en el ciberespacio e interacción



Los objetivos se diluyen en el ciberespacio, pero el objetivo 1 se hace más visible cuando interacciona y se mueve por Internet

La relación entre la mayor interacción de un sujeto en el ciberespacio con la probabilidad de ser victimizado podría darse por probada a partir de varios de los estudios empíricos de victimización en el ciberespacio:

- Así, **Alshalan** logra relacionar la victimización por virus informáticos, por una parte, y por otra, por cibercrímenes tales como el ciberfraude en sus múltiples formas, *identity theft*, *phishing*, fraudes de seguridad, *cyber-stalking*, *cyber-harassment*, extorsión y *hacking*, con la interacción de la víctima en el ciberespacio concretada en su frecuencia de acceso y el tiempo pasado en Internet. En efecto, y a partir de la hipótesis de que el comportamiento de la víctima en el ciberespacio es un importante predictor de su victimización, concluye que a mayor frecuencia de acceso a Internet, mayor riesgo de victimización; y lo mismo sucede con el mayor tiempo conectado en el ciberespacio, así como con la realización de actividades en Internet que conllevan la divulgación de datos personales de tipo financiero y, exclusivamente para la infección por virus, con el hecho de tener hijos que acceden al ciberespacio.

Uso frecuente de Internet

En un estudio de Ybarra y Mitchell, se relaciona de forma significativa el uso frecuente de Internet o el uso de salas de chat con una mayor exposición a la pornografía por parte de menores de edad, y ya hemos visto anteriormente que también había una intensa relación entre la interacción de la víctima en chats y demás con la victimización por *online grooming* o delitos similares.

- Por su parte, **Yucedal**, que examina los factores que inciden en la victimización por conductas de *spyware* y *adware*, concluye que el comportamiento cotidiano en relación con el uso de Internet es un elemento determinante de la victimización por estos delitos, que exigen, generalmente, que sea el propio sujeto el que al visitar una determinada web o al descargarse un programa, cargue involuntariamente el virus.

- Finalmente, **Choi** realiza una interesante identificación entre los comportamientos cotidianos en Internet y la teoría de los estilos de vida y la utilización de sistemas de protección con varios tópicos relacionados con la teoría de las actividades cotidianas. Llega a la conclusión, después confirmada por Yucedal, relativa a que el *hacking* es más factible en personas con ordenadores personales que utilizan mucho Internet y que realizan conductas de riesgo en línea. Y esto es así con otro tipo de cibercrímenes.

En el ciberespacio, por tanto, a mayor interacción de un sujeto, plasmada en mayor tiempo en línea o mayor variedad de actividades en Internet, mayor aptitud del mismo para ser objetivo adecuado. Es obvio que esto debe ser precisado y concretado de forma empírica y diferenciando cada una de las actividades. Pero también lo es que solo con la interacción se producirá el contacto (necesario para el delito) en el vasto ciberespacio entre el agresor motivado y la víctima; y que esto se produzca dependerá de que esta "se mueva" por Internet, especialmente si recordamos que muchos de los ataques en Internet quedan estáticos a la espera de que sea la propia víctima la que al entrar en la página o descargar el archivo, se convierta con su conducta en objetivo adecuado.

Ejemplo de actividades en red

Descarga de archivos, entrada en plataformas p2p, realización de compras en línea, creación de perfiles en redes sociales, etc.

Podemos concluir, pues, que las condiciones para la adecuación del objetivo del crimen VIVA no son transportables al ciberespacio, excepto en el caso del valor. Este deberá sumarse a la primera y esencial condición, y es que el objetivo haya sido introducido en el espacio virtual. A ellos deberá sumarse la Interacción del titular del objeto en el ciberespacio como esencial condicionante de la victimización.

Sumando las tres nos quedaría el acrónimo **IVI**, como definitorio de las condiciones que determinarán que una persona o alguno de sus bienes pueda ser objetivo adecuado de un cibercrimen:

- **Introducción**: que el bien o la persona haya sido introducido en el ciberespacio.
- **Valor**: que tenga un valor que lo haga apetecible para el cibercriminal.
- **Interacción**: que la persona con la titularidad del bien interaccione en Internet de forma que se haga en él visible y pueda contactar con el agresor motivado.

2.3.3. Guardianes capaces

El último elemento a analizar dentro de la teoría de las actividades cotidianas es el guardián capaz. La unión de los factores que hemos analizado, la compresión espacio temporal para la comunicación entre personas, la popularización y el nivel transnacional de dicho ámbito, etc., dificultan en el ciberespacio la actuación del guardián (que debe ser) capaz de proteger a la víctima, lo cual, a su vez, interacciona con el factor agresor motivado al percibir tal reducción de obstáculos y disminuir la percepción de riesgo de ser cazado que va a tener el (ciber)criminal.

La noción de guardián capaz se convierte en importante, pero también compleja, cuando pensamos en el cibercrimen. Quizás en este sentido sea más útil la diferenciación entre el mánager o gestor del lugar, y el guardián que opera directamente sobre la víctima o el objetivo potencial. La ausencia de mecanismos centrales de concesión de los servicios de Internet, así como de sistemas de control formal supranacional que tomen decisiones relativas a los servicios que estén por encima de las legislaciones estatales, conlleva la imposibilidad de unos "gestores centralizados" que vigilen el ciberespacio de forma global y así, protejan a las potenciales víctimas. No es que no haya policía en Internet, ni que no haya gestores de sitios en algunos de ellos, sino que los mismos están muy focalizados y su ámbito de incidencia es muy reducido, si bien es indudable que en determinados sitios web, como las redes sociales, los gestores pueden y deben funcionar tutelando la interacción de los usuarios de las mismas. Tales dificultades de gestión de un lugar tan vasto, por otra parte, son perfectamente conocidas por los usuarios de Internet, que perciben que "navegar por el ciberespacio" es una actividad en la que la intervención de los medios de control formal está mucho más diluida.

Distintos a los gestores del lugar son los guardianes de los objetivos adecuados. Estos lo pueden ser cualesquiera otros sistemas personales o no, ajenos a la propia víctima o impuestos por ella misma, que sirvan como forma de protección. Al igual que los sistemas de seguridad físicos, tales como alarmas, cerrojos especiales, etc. se han mostrado eficaces frente a la criminalidad, también pueden serlo aquellos otros que ejercen la misma función en el ciberespacio, tales como los antivirus o cualesquiera otros sistemas de seguridad. Los estudios empíricos demuestran que tales sistemas pueden ser muy eficaces para evitar la victimización por el cibercrimen. Pero se trata, en todo caso, de unos guardianes capaces, íntimamente ligados con el elemento objetivo adecuado: no son sistemas de protección incorporados o que funcionen de forma autónoma al comportamiento del propio sujeto al que protegen, sino que, por el contrario, todos los elementos de protección citados dependen de la propia víctima para su funcionamiento y actualización. Los que Cohen y Felson definían como guardianes capaces generalmente eran cercanos a la víctima (vecinos, ciudadanos anónimos, etc.), pero no "parte de ella", como sí lo es el software que la víctima pone en su ordenador. En el caso del ciberespacio, es la propia víctima, por tanto, el propio objetivo, quien debe incorporar sus guardianes capaces. Por lo tanto, el guardián capaz en el ciberespacio es prácticamente un autoguardián que depende de la propia víctima.

Es cierto que los sistemas de autoprotección impuestos por la víctima no son los únicos que pueden desarrollar su eficacia en relación con los cibercrímenes. En otros delitos dirigidos contra menores, pueden ser interesantes otros vigilantes capaces como son el control familiar sobre la actividad en Internet, la creación de perfiles específicos que impidan el acceso a determinados recursos web, etc. A ello deberán sumarse en el futuro, medios de control y protección institucional, dado que la seguridad en el ciberespacio exige una intervención y esfuerzo plural de instituciones y usuarios. En todo caso, esto parece más lejano.

Ante la inexistencia actual de medios de control formal más institucionalizados, como las fuerzas policiales, cuya función preventiva (que no la reactiva) parece imposible en el ciberespacio, la autodefensa sigue siendo, frente a estos crímenes, como quizás también frente a los otros, la mejor forma de protección.

3. El rol de la víctima para la prevención del ciberdelito

Generalmente, el elemento central para la visión y comprensión del crimen es el agresor, dado que en su motivación está también definido el objetivo sobre el que se producirá el ataque y las condiciones de defensa que tiene el mismo. Esto podría hacer pensar que el agresor elige completamente a su víctima independientemente del actuar de esta y que, para ella, el serlo es algo aleatorio. Pero si eso no es así en el espacio físico, aún parece serlo menos en la cibercriminalidad. Son muchos los ciberataques que se realizan en el ciberespacio sin un objetivo determinado, siendo el concreto interactuar de la víctima el que la convierte en objetivo adecuado y no la voluntad del cibercriminal, y esto es así porque el ciberespacio es un ámbito de oportunidad nuevo (distinto).

La principal diferencia de la botella del crimen en el ciberespacio es que, debido a que el mismo es un ámbito comunicativo vasto e inmenso, sin barreras ni dimensiones, en el que el contacto depende de las voluntades de interacción entre sujetos, de modo tal que sin interacción de los dos no habrá contacto por más que uno quiera, el agresor ya no es el único y principal que define, desde su intención, el ámbito de riesgo. Lo hace, sin duda, al actuar con una voluntad criminal, pero lo hará únicamente sobre aquel objeto (para él valioso) que esté en el ciberespacio, que interaccione con él y que no esté protegido, todo lo cual convierte a la víctima en un elemento explicativo (*a posteriori*) del evento delictivo muy expresivo.

Son tres los factores que hacen que la víctima adquiera una especial importancia para la explicación y prevención del delito en el ciberespacio:

- El primero, como se ha visto, es que la víctima potencial del ciberdelito tiene, en primer lugar, gran capacidad para dejar fuera del ámbito de riesgo aquello que no quiere que se vea afectado por el mismo: ella misma determina, desde un primer momento, al incorporar determinados bienes y esferas de su personalidad al ciberespacio, los márgenes genéricos del ámbito de riesgo al que va a estar sometida. Si no entra en el ciberespacio o no tiene relaciones personales allí, tales bienes no podrán ser afectados, al igual que no lo podrá ser su patrimonio si no utiliza la banca electrónica y no comunica sus claves en Internet. Podría decirse que esto es idéntico a que si la víctima no sale a la calle no puede ser víctima de robos en ella.

- En segundo lugar, la víctima define con su interacción en el ciberespacio el grado de visualización de sus objetivos y, por tanto, las posibilidades de contacto con un agresor motivado en un mismo tiempo y espacio o en otro distinto. Existen estudios que demuestran la especial importancia del comportamiento de la víctima en la victimización por la cibercrimina-

lidad informática. Todos ellos vienen a confirmar algo que ya habíamos afirmado: que la víctima define el ámbito de riesgo al que puede acceder el agresor motivado. Podría argumentarse que esto no es más que lo que sucede en el espacio físico, con el aumento de las posibilidades de sufrir delitos en el caso de visitar determinados lugares, hacerlo en determinados periodos del día, etc. Ciertamente es similar, pues se basa en que las actividades cotidianas de la víctima son parte de la explicación del evento criminal. La única diferencia es que en el ciberespacio no es necesario tiempo ni distancia física para la interacción, y que la misma en Internet depende por igual de todos los agentes, de modo que una vez hay una conducta criminal iniciada, que la misma afecte a uno, dos, cientos o miles de personas dependerá mucho de lo que hagan estas.

- Por último, y en tercer lugar, la víctima va a ser prácticamente la única que puede incorporar guardianes capaces para su autoprotección. Al no existir en este ámbito criminológico distancias físicas ni guardianes formales institucionalizados, el uso cotidiano que haga de las TIC y en especial la incorporación (o no) de sistemas digitales de autoprotección, serán determinantes a la hora de convertirse en víctima del cibercrimen. Si tenemos en cuenta, además, que en Internet, al no existir tampoco distancias, el desplazamiento del cibercriminal hacia otros objetivos resulta no solo sencillo, sino incluso en muchos casos (virus y demás) instantáneo, y que la dirección del nuevo objeto del ataque la marcará la ausencia de sistemas de protección o las vulnerabilidades del objetivo (entonces adecuado), parece evidente concluir el protagonismo de la víctima en su proceso de autoprotección y, en caso de carecer de esta, de victimización.

Todo lo anterior se resumiría, por tanto, en que si la conducta de la víctima va a ser un determinante especialmente significativo del delito, también será, por ello, un importante condicionante para su prevención. La educación de la víctima en seguridad informática, su concienciación para la adopción de software de protección y de rutinas seguras en su actuar cotidiano en el ciberespacio, así como la información real sobre los riesgos en el ciberespacio, serían los primeros pasos a adoptar para la prevención del cibercrimen.

4. La prevención situacional del ciberdelito

Una vez estudiadas las características del ciberespacio y haber determinado este como un ámbito de oportunidad, así como la importancia del hacer de la víctima para delimitar su ámbito de riesgo, el siguiente paso para concluir el temario, es hacer un breve repaso a las medidas que se pueden llevar a cabo para prevenir el cibercrimen.

Partiendo de la teoría de las actividades cotidianas, si no hay agresor motivado o hay guardián capacitado no habrá delito *online*, independientemente de lo que haga la víctima o el titular del "objetivo adecuado". Pero dado que hay pocos gestores del sitio, así como guardianes capaces en Internet y que la compresión de la distancia sitúa en un mismo plano a miles de potenciales agresores motivados, parece obvio que la conducta de la víctima determinará significativamente el riesgo criminal al que esté sometida. Lo hará desde el momento de su entrada en el ciberespacio, con la selección de los bienes patrimoniales y relacionados con la privacidad, contenidos en su sistema informático y que entran en ese espacio de riesgo nuevo; también al elegir el tipo de actividades que realiza en Internet (sociales, personales, económicas) y al decidir los lugares que visita, los contactos personales que realiza, los archivos que descarga, y, muy especialmente, los medios tecnológicos (software antivirus, *firewalls* y demás sistemas de protección y de detección de accesos no autorizados, de la entrada de software malicioso y de demás ataques; pero también los sistemas de control parental, etc.) que incorpora a su sistema informático como autoguardianes para la protección de sus datos y demás.

No obstante, partiendo de las premisas de la prevención situacional, que pone el énfasis en la importancia de los factores ambientales, además de trabajar con los aspectos más relacionados con la víctima, se puede intervenir en las características que conforman el ciberespacio que hacen de este un nuevo ámbito delictivo, para reducir la delincuencia con una serie de medidas sobre las que se puede incidir, como veremos a continuación:

1) El primer bloque de medidas está destinado a reducir el ámbito de incidencia, entre las que se incluyen cuatro medidas específicas:

- **No introducción de objetivos**. La primera de las medidas, y a su vez la más significativa, es la no introducción de objetivos. Se trataría de que el usuario, víctima potencial, no ponga a disposición de terceros bienes o información que, mediante técnicas como la minería de datos, pueden

aportar a los ciberdelincuentes información con la que organizar sus ciberataques, o bien impidiéndole a la propia víctima que descargue archivos que pueden estar infectados de virus (controladores de seguridad ActiveX) o que, mediante los distintos sistemas de filtrado de contenidos, acceda a webs en las que se difunde material peligroso, lo cual, en el caso de los menores, se concreta en las distintas formas de software de control parental.

- **Separación de objetivos en el ciberespacio**. La segunda medida es la separación de objetivos en el ciberespacio, que podría verse plasmado con la creación de ciberespacios cerrados y separados de la Red (un ejemplo de ello es Internet2).

- **Identificación de riesgos**. La tercera medida es la identificación de riesgos por parte de los usuarios y que podría realizarse mediante campañas de información sobre los peligros que implica la exposición a determinados ámbitos del ciberespacio (descarga de contenidos con derechos de autor, apoyo a grupos de ciberactivistas, las webs de pornografía, etc.).

- **Descontaminación de residuos**. Finalmente, la descontaminación/limpieza de residuos, como el borrado de virus latentes. Esta acción impedirá el crecimiento ilimitado de los peligros de Internet, que, como una enfermedad supuestamente extinta que encontrase un nuevo portador, aumentaría su virulencia extendiéndose en progresión geométrica.

2) El segundo bloque de medidas trata de aumentar el esfuerzo percibido por el ofensor motivado:

- **Control de acceso a los sistemas**. Se incluirían, por tanto, en primer lugar las medidas destinadas a controlar el acceso a los sistemas, con la incorporación por parte de la víctima potencial, de cortafuegos, claves de acceso al sistema y a las redes, así como su renovación periódica, la actualización de sistemas operativos, etc.

- **Detección del ataque**. En segundo lugar se incluyen medidas que, una vez que la víctima es atacada, lo detecten e impidan que el ataque finalice con éxito. Para ello están todos los sistemas antivirus que intervienen una vez la infección se ha producido y que tratan de identificar la amenaza, de bloquearla y finalmente, de eliminarla. En sentido similar actúan los programas *antispyware* frente al software que no infecta nuestro sistema pero trata de adquirir información valiosa (*keyloffers*, *sniffers* y demás) y que son bloqueados por este tipo de *software* defensivo. En cuanto al *antispam*, se trata de un tipo de software que filtra los correos electrónicos detectando la entrada de correos *spam* y ubicándolos en la carpeta de *spam*.

- Otra medida que puede aumentar el esfuerzo percibido es que el trasgresor sea retirado, aunque sea temporalmente, de modo que tenga que volver a

empezar para perpetrar el ataque. Esto puede hacerse de distintas formas en el ciberespacio mediante:

– Cierre de páginas web por parte de las autoridades estatales competentes.

– Solicitud de retirada de contenido ilícito como primer paso para el cierre de la web.

– Mecanismos de denuncia en redes sociales que permiten que un contenido o una web sea retirada inmediatamente por el controlador de la red social, o cortando el acceso a una determinada IP, identificada previamente como peligrosa. Este tipo de medidas pueden lograr temporalmente el objetivo final, pero en cualquier caso, el agresor tiene que volver a empezar lo que supone una reiteración de esfuerzo.

– Por último, quedaría controlar aquellos elementos que hacen más sencilla la comisión del delito. Se refiere a medidas, como que los prestadores de servicio tengan obligaciones de vigilancia o que las redes sociales controlen mejor el acceso a los datos personales de los usuarios.

Otras formas de detección de ataques

Junto a los antivirus y los programas *antispyware* que se pueden instalar en el propio sistema para la autoprotección de este, hay otras formas de detección del ataque que tienen lugar cuando el mismo ya se ha producido contra el usuario pero aún no se ha perfeccionado por completo, pudiendo ser identificado por el vigilante-víctima para evitar que termine teniendo éxito. Es lo que ocurre con los sistemas de protección de la banca electrónica, que vigilan no solo el acceso a las cuentas, sino incluso la legalidad de la misma, una vez se ha producido una transferencia, antes de que el dinero sea definitivamente retirado.

3) El tercer grupo de medidas tiene como objetivo aumentar en el agresor la percepción de que su conducta entraña para él un riesgo, concretamente el de ser detenido:

- **Nuevos guardianes**. Las primeras medidas irán encaminadas a aumentar el número de guardianes. No es el ciberespacio un ámbito en el que existan guardianes formales derivados de una autoridad centralizada, pero sí que existen otro tipo de vigilantes en lugares concretos, tales como las redes sociales o los foros de Internet, moderadores que actúan en ellos y que pueden vigilar la realización de expresiones injuriosas o de proposiciones sexuales y otras actividades de acoso. Junto a ello, también existen otros sistemas de vigilancia, cuya legitimidad, sin embargo, es más discutida. Se trata de aquellos sistemas de inteligencia, tales como Echelon o su equivalente europeo Enfopol, que de forma no oficial captan todas las transmisiones de información realizadas por medio de redes telemáticas con selección de términos y conceptos clave y que podrían estar violando la intimidad de las personas de forma fragrante.

- **Reducción del anonimato**. Luego se incluyen todas aquellas que tratan de reducir el anonimato con el que este generalmente actúa. Se podría con-

seguir mediante el registro previo con la utilización de datos personales, como ya se hace en algunas webs y redes internas que exigen a los usuarios una identificación con datos o claves personales en el ámbito institucional estatal, en el empresarial, educativo, social y demás. Más sofisticada y lejana, pero no imposible dadas las experiencias existentes en otros medios, sería la implantación de sistemas de identificación y autentificación biométricos, entre las que podrían estar el reconocimiento facial, el reconocimiento de huellas dactilares, el escáner de la geometría de la mano o el reconocimiento del iris, etc.

- **Reforzamiento de la vigilancia formal**. Otras medidas dirigidas a incrementar el riesgo percibido por el criminal en el espacio físico son el reforzamiento de la vigilancia formal y la introducción de gestores de sitios. Aunque no exista una autoridad centralizada en el ciberespacio, los distintos estados están obligados a investigar y perseguir la criminalidad que allí se produce y que puede dañar los bienes jurídicos de sus nacionales, y por ello, cada vez más utilizan los medios tecnológicos para la vigilancia del ciberespacio por medio de equipos especializados de persecución de este tipo de delincuencia. En la actualidad, la intervención policial frente a la cibercriminalidad se centra en la persecución de la pornografía infantil en Internet, tanto de las páginas que se dedican a la distribución de este material como de quienes poseen este tipo de material prohibido.

- **Mejora de los sistemas de vigilancia**. Por último, y como medidas complementarias a las anteriores, también es posible la aplicación de medidas tendentes a facilitar los medios de vigilancia, a mejorarlos para una mayor eficacia. En este sentido, la mejora de la identificación de las direcciones IP y en general la mejora de los sistemas de detección de la huella digital, serían esenciales para la identificación de los infractores. Como medidas de facilitación de los medios de vigilancia también se suele citar la mejora del diseño del espacio para hacerlo más defendible.

Contraataques

Y a estas cuatro clases de medidas se añade últimamente otra no institucionalizada, pero que sin duda es tomada en consideración por algunos tipos de cibercriminales. Se trata del aumento de los riesgos derivados de la realización de ilícitos en Internet que no consisten en ser detenido o enjuiciado, sino en ser víctima de daños o ataques a sus sistemas a causa del realizado por ellos. Esto ocurre con algunas formas de *hacking*, que llevan aparejadas contraataques de los sistemas que se defienden infectando al sistema agresor, pero muy especialmente, con algunas conductas ilícitas relacionadas con los derechos de autor, dado que algunos de los archivos compartidos que aparentemente contienen obras del ingenio más bien son virus en ocasiones cargados por los interesados en que tales sitios web no prosperen y que pueden causar graves daños al sujeto que se los descarga.

4) El cuarto grupo de medidas trata de disminuir las ganancias que el agresor percibe que obtendrá de su conducta criminal:

- **Ocultación los objetivos**. En primer lugar hay formas de ocultar los objetivos a los "ojos" del agresor motivado. Se puede hacer mediante la utilización de sistemas de encriptación, y debe hacerlo la propia víctima en

las redes sociales si no quiere compartir tal información con otros. También es conveniente la no utilización de las claves bancarias, números de cuenta y demás datos necesarios para la final defraudación en Internet, en el ciberespacio, ni por correo electrónico ni en otros sistemas de envío telemático. Por último, una eficaz forma de ocultación de los objetivos puede constituir en general el perfeccionamiento de los sistemas de pago por Internet, que permitan la no utilización de claves o datos bancarios o, incluso, la exigencia de otro tipo de información que no suele ser necesaria para las transacciones comerciales, tales como los números impresos en la tarjeta y demás.

- **Desplazamiento de objetivos**. Otra forma de disminuir las ganancias percibidas es desplazando objetivos. En Internet el desplazamiento debe entenderse en un sentido distinto al tradicional de movimiento del objeto, cubriendo una determinada distancia, más bien como cambio en la ubicación electrónica en la que algo está contenido hacia un ámbito nuevo dentro del ciberespacio (incluso fuera, aunque entonces estaríamos más cerca de la retirada del objetivo). Así, será conveniente en ocasiones realizar un cambio en las direcciones web, direcciones de dominio y demás con una finalidad defensiva, como también utilizar discos duros distintos en un mismo sistema para tener separada y más protegida la información, e incluso en discos duros extraíbles, en el caso de que se trate de información confidencial que puede utilizarse y retirarse cuando se accede al ciberespacio. También se desplazan los objetivos cuando se crean sistemas de pago alternativos a los tradicionales (sistemas bancarios de tarjeta de crédito, etc.). Con ello lo que se logra es que un objetivo sea, por sí mismo, menos apetecible.

- **Eliminación de beneficios**. El ataque cibercriminal puede ser combatido eliminando los beneficios que el agente obtiene del mismo, influyendo así en la valoración sobre las posibilidades futuras de obtención de ganancias por tales conductas. En la cibercriminalidad económica, es importante la persecución de quienes permiten obtener los beneficios al delincuente. En el caso de la pornografía infantil, esto se puede lograr con la punición de la tenencia de estos materiales, de forma tal que al sujeto que decide poseer ese material pagando al que lo distribuye le cueste más la decisión al incrementar el perjuicio que puede derivarse de tal hecho. Del mismo modo, y dado que la mayoría de los cibercrímenes económicos son llevados a cabo por bandas organizadas, la persecución del blanqueo de capitales de estas organizaciones criminales puede ser de gran eficacia.

- **Fomento de medios lícitos**. Por último, se trata de hacer atractivos y más rentables los medios lícitos. Esto sería especialmente útil en intercambios de material protegido por los derechos de propiedad intelectual, por ejemplo, potenciando formas de distribución lícita y hacer poco rentable para

el consumidor el hecho de acceder al mercado ilegal cuando por poco precio se obtiene un mejor producto en el mercado legal.

5) El último grupo de medidas van encaminado a eliminar las excusas o justificaciones morales, incrementando, por tanto, los sentimientos de vergüenza o culpabilidad en el delincuente:

- **Fijación de reglas**. Para ello, es importante la fijación de reglas que pueden ser normas jurídicas, puesto que hay sectores de la población que dan valor ético a lo normativo, o también reglas sociales que respondan a la moral colectiva. En este sentido, es importante en el ciberespacio el fortalecimiento de reglas del buen uso de Internet, que servirán para que quien acceda a ese nuevo ámbito de comunicación social comprenda sus usos básicos, su funcionamiento aceptado por la sociedad que lo conforma. Además, sería recomendable la armonización del derecho que regula el ciberespacio a nivel internacional, pues en caso contrario siempre se puede utilizar la "excusa" de que en este otro país no se sanciona tal comportamiento.

- **Respeto del *copyright* o del *copyleft***. Es importante también que en las páginas web se incluyan referencias claras a las licencias *copyright* o *copyleft* y demás, así como avisar en las redes sociales sobre la privacidad de las imágenes y otros elementos personales de los usuarios de las mismas.

- **Refuerzo de actitudes positivas**. Otra forma de concienciación es el refuerzo de las actitudes positivas, en este caso de los negocios lícitos, en aras del debilitamiento moral de los que no lo son.

- **Fomento del comportamiento lícito**. Finalmente, dentro de esta categoría se pueden incluir medidas que faciliten el comportamiento lícito, como la creación de competiciones legales para *hackers* o el propio fortalecimiento y difusión del software libre como forma de fomento de la modificación y evolución de los sistemas informáticos, que servirían para que muchas personas siguieran realizando sus actividades en el ciberespacio pero de forma lícita.

Resumen

El ciberespacio es un ámbito virtual con dimensiones espacio-temporales distintas al mundo físico y caracterizado por la transnacionalidad, la neutralidad, la universalización del medio, su popularización en todas las sociedades y estratos, sujeto a revolución permanente, que otorga facilidades para el anonimato y presenta dificultades para la persecución de las actividades criminales.

Todo esto hace que la víctima adquiera un protagonismo mayor en el proceso de victimización. Como hemos visto, la víctima define su propio ámbito de oportunidad criminal dado que ella misma determina desde un primer momento, al incorporar determinados bienes y esferas de su personalidad al ciberespacio, los márgenes genéricos del ámbito de riesgo al que va a estar sometida y dado que, además, al no existir en este ámbito criminológico distancias físicas ni guardianes formales institucionalizados, el uso cotidiano que haga de las TIC y en especial la incorporación (o no) de sistemas digitales de autoprotección serán determinantes a la hora de convertirse en víctima del cibercrimen. Si tenemos en cuenta, además, que en Internet, al no existir tampoco distancias, el desplazamiento del cibercriminal hacia otros objetivos resulta no solo sencillo sino incluso en muchos casos (virus y demás) instantáneo, y que la dirección del nuevo objeto del ataque la marcará la ausencia de sistemas de protección o las vulnerabilidades del objetivo (entonces adecuado), parece evidente concluir el protagonismo de la víctima en su proceso de victimización.

Para combatir este tipo de delincuencia a partir del análisis de las teorías de la oportunidad delictiva, se proponen una serie de medidas generales, según las cuales se establecerán medidas más concretas. Estas medidas pasan por una mayor formación de los usuarios para la adopción de rutinas seguras, así como potenciar la utilización de sistemas de autoprotección, la implantación de guardianes capaces en el ciberespacio, trasladar al ciberespacio sistemas de prevención comunitaria informal e influir en la decisión del agresor motivado para que finalmente no cometa el delito.

Ejercicios de autoevaluación

1. En el ciberespacio:

a) Las distancias se expanden y la comunicación, por tanto, se expande.
b) Las distancias se contraen y, por lo tanto, las posibilidades de comunicación se reducen.
c) Las distancias se contraen y, por lo tanto, la comunicación se expande.
d) Todas las opciones de respuesta son falsas.

2. Para que un objetivo sea considerado adecuado en el ciberespacio…

a) ha de ser introducido y tiene que tener valor.
b) tiene que interaccionar para pasar desapercibido.
c) ha de tener siempre valor económico.
d) ha de ser introducido, tiene que interaccionar y ha de tener valor.

3. ¿Cuál de las siguientes características no es configuradora del ciberespacio?

a) Localizado.
b) Anonimizado.
c) Neutral.
d) Universal.

4. Desde una postura mixta, el cibercrimen…

a) es idéntico estructuralmente al delito cometido en el espacio físico, cambiando únicamente el aspecto del mismo, pero no sus caracteres configuradores.
b) comparte con la delincuencia todos los elementos definitorios del concepto de "crimen", pero dándose los mismos de una forma tal en el nuevo ámbito que es el ciberespacio, que puede influir significativamente en la explicación del delito.
c) es un tipo de delincuencia nueva, para la cual no son válidas las teorías tradicionales creadas para explicar el espacio físico.
d) es un tipo de delincuencia nueva pero se pueden aplicar las mismas teorías creadas para el espacio físico.

5. Señalad la respuesta correcta:

a) En el ciberespacio no existen barreras para la comunicación e interacción entre individuos.
b) El ciberespacio está situado en un sitio concreto pero en un sentido funcional está en todos a la vez.
c) En Internet no existen nodos centrales pero sí nodos que actúan como centros locales.
d) El usuario de Internet puede navegar por el ciberespacio a cualquier hora pero no puede acceder a todas las zonas del ciberespacio.

6. El enfoque de las actividades cotidianas explica a nivel micro el evento criminal. Para que se produzca un delito deben coincidir en el espacio…

a) un objetivo adecuado y un agresor motivado.
b) un delincuente motivado y un guardián capaz.
c) un agresor motivado y un objetivo adecuado con la ausencia de un guardián capaz.
d) un agresor motivado y un objetivo adecuado con la presencia de un guardián capaz.

7. Desde la perspectiva de la teoría de las actividades cotidianas, podríamos considerar como un objetivo adecuado…

a) las víctimas.
b) las víctimas y el objeto del delito.
c) el objeto del delito.
d) Ninguna de las respuestas es correcta.

8. Un agresor en el ciberespacio…

a) puede atacar a varias personas con una única conducta.
b) puede atacar desde el lugar físico en el que se encuentra y que los efectos de su ataque se produzcan a miles de kilómetros de distancia.
c) puede realizar un ataque y que los efectos no se desplieguen al momento.
d) Todas las opciones anteriores son correctas.

9. Señalad la afirmación correcta:

a) La introducción de un objetivo en el ciberespacio no siempre es voluntaria.
b) En el ciberespacio es difícil pasar desapercibido.
c) El cibercrimen tiene costes de desplazamiento y de huida para el agresor.
d) El cibercrimen no tiene coste temporal.

10. El actuar de la víctima es importante de cara a la prevención porque…

a) puede dejar fuera del ámbito de riesgo aquello que no quiere que se vea afectado.
b) define con su interacción en el ciberespacio el grado de visualización de sus objetivos.
c) puede incorporar guardianes capaces para su autoprotección.
d) Todas son correctas.

Solucionario

Ejercicios de autoevaluación

1. c

2. d

3. a

4. b

5. a

6. c

7. b

8. d

9. a

10. d

Glosario

adware *m* Programas autoejecutables, que, generalmente sin conocimiento ni consentimiento del usuario, muestran publicidad en el ordenador al instalarse o al interaccionar con determinadas webs, y que pueden servir para espiar sus hábitos en Internet.

antispyware *m* Aplicación que se encarga de buscar, detectar y eliminar espías en el sistema.

bot *m* Tipo de virus que permite el acceso remoto del sistema informático a través de la Red.

IP (protocolo de Internet) *m* Es un código empleado en redes de comunicaciones para identificar de forma inequívoca la procedencia de una conexión.
en Internet protocol

IRC *m* Programa que permite desarrollar conversaciones en línea en tiempo real con gente de todo el mundo escribiendo mensajes por Internet.
en Internet relay chat

ordenador zombie *m* Denominación que se asigna a ordenadores personales que tras haber sido infectados por algún tipo de *malware*, pueden ser usados por una tercera persona para ejecutar actividades hostiles.

spyware *m* Virus que captura información de los sistemas informáticos.

TCP (protocolo de control de transmisión) *m* Uno de los protocolos fundamentales en Internet.
en Transmission control protocol

Wifi *f* Tecnología de comunicación inalámbrica.

WWW *f* Iniciales que identifican a la expresión en ingles World Wide Web, literalmente, red informática mundial, es la red global mundial de intercambio de documentos a través de hipertexto comúnmente conocida como Internet.

Bibliografía

Aguirre Romero, J. Mª (julio-octubre, 2004). "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI". *EREL* (núm. 27). Universidad Complutense de Madrid. Disponible en http://www.ucm.es/info/especulo/numero27/cibercom.html.

Alcantara, J. (2011). *La neutralidad en La Red, y por qué es una mala idea acabar con ella*. Madrid: Biblioteca de Las Indias.

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of A National Survey*. Mississipi: Mississippi State University.

Bossler, A. M.; Holt, T. J. (enero-junio, 2009). "Online Activities, Guardianship, and Malware Infection". *IJCC* (vol. 3, núm. 1).

Brantingham, P. J.; Brantingham, P. (2001). "The implications of the criminal event model for crime prevention". En: R. F. Meier; L. W. Kennedy; V. F. Sacco (eds.). *The Process and structure of Crime. Criminal events and crime analysis*. New Jersey: Transaction Publishing ("ACT", vol. 9).

Castells, M. (2006). *La era de la información. Vol. 3. Fin de milenio*. Madrid: Alianza.

Choi, K. (enero-junio, 2008). "Computer Crime Victimization and Integrated Theory: An Empirical Assessment". *IJCC* (vol. 2).

Clarke, R.; Felson, M. (eds.) (1993). "Routine activity and rational choice". New Brunswick, New Jersey: Transaction Publishers ("ACT", vol. 5).

Cohen, L.; Felson, E. (1979). "Social change and crimen rate trends: a routine activity approache". *ASR* (vol. 44).

Cornish, D. V.; Clarke, R. V. (2003). "Opportunities, precipitator and criminal decisions: A reply to Wortley's critique of situational crime prevention". En: M. Smith; D. B. Cornish (coords.). *Theory for Practice in Situational Crime Prevention.CPS* (vol. 16). Nueva York/Monsey: Criminal Justice Press.

Grabosky, P. (2001). "Virtual Criminality: Old Wine in New Bottles?". *SLS* (núm. 10).

Graham, P. W. (2002). "Space and Cyberspace: on the enclosure of consciousness". En: J. Armitage; J. Roberts (eds.). *Living with cyberspace: technology & society in the 21st century*. Londres: Continuum International Publishing Group.

Gutiérrez Puebla, J. (1998). "Redes, espacio y tiempo". *AGUC* (núm. 18).

Kitchin, R. M. (1998). "Towards geographies of cyberspace". *PHG* (vol. 22, núm. 3).

Medina Ariza, J. J. (1998). "El control social del delito a través de la prevención situacional". *RDPC* (2.ª época, núm. 2).

Miró Llinares, F. (2011). "Cibercrímenes económicos y patrimoniales". En: I. Ortíz de Urbina Gimeno (dir.). *Memento práctico penal y económico de la empresa 2011-2012*. Madrid: Francis Lefebvre.

Miró Llinares, F. (2011). "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen". *RECPC* (núm. 13-07). Disponible en http://criminet.ugr.es/recpc/13/recpc13-07.pdf.

Miró Llinares, F. (2005). *Internet y delitos contra la propiedad intelectual*. Madrid: Iberautor Promociones Culturales.

Pease, K. (2001). "Crime futures and foresight: Challenging criminal behaviour in the information age". En: D. Wall (ed.). *Crime and the Internet*. Londres: Routledge.

Serrano Maíllo, A. (2009). *Oportunidad y delito*. Madrid: Dykinson.

Serrano Maíllo, A. (2009). *Introducción a la criminología* (6.ª ed.). Madrid: Dykinson.

Yar, M. (2005). "The novelty of 'cybercrime': an assessment in light of routine activity theory". *EJC* (núm. 2).

Ybarra, M. L.; Mitchell, K. (2005). "Exposure to Internet Pornography among Children and Adolescents: A National Survey". *CpB* (vol. 8, núm. 5).

Yucedal, B. (2010). "Victimization in cyberspace: An application of routine activity and lifestyle exposure Theories". Disponible en http://etd.ohiolink.edu/send-pdf.cgi/yucedal%20behzat.pdf?kent1279290984.