Victimología:

¿Qué sabemos sobre las víctimas de delitos para poder intervenir adecuadamente?

MÓDULO IV: PROCESOS DE VICTIMIZACIÓN Y RECUPERACIÓN VICTIMAL EN DIFERENTES TIPOS DE DELITOS (II)

(Ana I. Pérez Machío)

EPISODIO IV. Procesos de victimización en el ámbito de la ciberdelincuencia

La contribución de la víctima a la comisión del ciberdelito.

Desde una perspectiva victimológica, diversas teorías han resaltado que la conducta de la víctima no es un elemento neutro, si se busca una explicación al delito.

La cibercriminalidad se presenta, a este respecto, como una modalidad de delincuencia ocupacional que se concentra en particulares espacios y se vincula a las oportunidades existentes en los mismos. Como algunos autores vienen destacando, los delincuentes adoptan diferentes decisiones a la hora de cometer el delito y estas decisiones están basadas en su conocimiento previo de lo que constituyen buenos objetivos o víctimas. De esta forma, cuando el delincuente identifica una buena oportunidad criminal, es cuando se dan las condiciones para que el mismo decida cometer el delito. Es por lo tanto la nota de oportunidad el elemento común a un fenómeno criminal que se vincula a la oportunidad del mismo.

Pues bien, en esta forma de entender el fenómeno criminógeno, en cuanto delincuencia ocupacional vinculada a la oportunidad del mismo, destaca la contribución de la víctima a la comisión del concreto delito.

Las teorías del control social tradicionalmente han servido para explicar la racionalidad espacial y temporal de lo que se viene conociendo como delincuencia común, incidiendo en el papel que el espacio y los lugares desempeñan en la

distribución del delito. Pues bien, frente a las teorías del control social que explican el fenómeno de la Cibercriminalidad a partir de la contribución de las propias víctimas, surgen las teorías de la prevención situacional, cuyo objetivo es influir en las actitudes de las potenciales víctimas con la finalidad de reducir las oportunidades delictivas y hacer más difícil la comisión del delito. La teoría situacional reposa en una teoría individual de elección racional de los agresores, que presupone que los delincuentes son, hasta cierto punto, racionales y que consideran muchos factores antes de cometer un acto delictivo, como pueden ser: las características de la víctima, los riesgos de ser descubiertos, la disponibilidad de los objetivos, las posibles ganancias, el tiempo requerido, el peligro físico, la pericia que se necesita y la familiaridad con el método. Pues bien, frente a esta realidad de oportunidades situacionales que favorecen la comisión del delito, las teorías de la prevención situacional proponen una serie de medidas de reducción de oportunidades, que se reconducen a tres grupos.

En primer lugar, medidas que incrementan el esfuerzo necesario para cometer un delito, entre las que destacan: el endurecimiento de objetivos (barreras físicas, cualquier estrategia de protección); control de acceso (contraseñas); desviación de transgresores (evitar la acumulación de personas conflictivas en el mismo lugar y a la misma hora); control de facilitadores (armas de fuego).

En segundo lugar, medidas que incrementan el riesgo, como por ejemplo: control de entradas y salidas, vigilancia formal, vigilancia por empleados, vigilancia natural

Y, en tercer lugar, estrategia de reducción de ganancias.

Pues bien, las medidas de reducción de oportunidades de las teorías de la prevención situacional tienen perfecto acomodo en la prevención de la delincuencia informática, habida cuenta de la estrategia de oportunidades reales para el delincuente y la “contribución” de la víctima a este fenómeno criminógeno.

La cibercriminalidad, vinculada, como se acaba de poner de manifiesto, a la racionalidad espacial del delito a la que contribuyen las enormes oportunidades que determinados sistemas operativos ofrecen a los delincuentes informáticos, deriva de

las conductas de sus víctimas. En efecto, en el concreto ámbito de la cibercriminalidad los análisis empíricos tradicionalmente han venido mostrando que la mayoría de los casos de delincuencia informática se causa, se permite o, como mínimo, se simplifica, por la ineficacia o carencia de sistemas de seguridad.

Desde esta perspectiva, las víctimas favorecen y motivan la delincuencia informática, dotando a los autores de las mismas oportunidades reales que una y otra vez facilitan la comisión de todo tipo de ilícitos cibernéticos. La no adopción de sistemas de seguridad o de controles informáticos y el acceso público gratuito de un nutrido grupo de personas (normalmente trabajadores) a determinados sistemas operativos con una misma clave común, son situaciones que evidencian tanto la fragilidad de muchos de los sistemas informáticos de las grandes empresas y de los usuarios particulares, como la oportunidad espacial de la comisión de un concreto delito informático.

Bastaría, en este sentido, con que las potenciales víctimas (empresas, particulares) adoptaran medidas preventivas adecuadas para la seguridad del sistema informático que permitieran disuadir al potencial delincuente cibernético de la comisión del ilícito: incrementando el esfuerzo necesario para cometer el delito (mejorar los sistemas de seguridad del sistema operativo; asignando a todos los usuarios de ordenadores una clave personal de acceso; impidiendo el acceso público y libre; impidiendo que exista un ordenador de uso común para una pluralidad de sujetos sin clave personal); incrementando el riesgo (vigilancia de las entradas y salidas a los sistemas operativos; existencia de un especialista en materia de seguridad informática y de delincuencia informática que asesore en las empresas sobre esta realidad); y, por último, en la medida de lo posible, implantando de estrategias de reducción de ganancias que, si bien tradicionalmente se han venido asociando al desplazamiento de objetivos, en el caso específico de la cibercriminalidad, puede relacionarse con las modificaciones de cuentas corrientes -supuestos de estafa informática- y con los cambios continuos de las claves de acceso a modo de protección del potencial objeto material del delito.

A pesar de la efectividad que parece derivarse de las medidas vinculadas a la teoría de la prevención situacional, éstas tradicionalmente no han estado exentas de

críticas en un doble sentido. Por un lado, vinculando este paradigma de prevención con un modelo de sociedad clasista en la que los ciudadanos con medios económicos suficientes se protegerían con innumerables medidas de seguridad, frente a una gran masa poblacional que carecería de recursos suficientes para lograr dichas cotas de protección; y, por otro, considerando que la teoría de la prevención situacional sólo puede servir para frenar la conducta delictiva convencional (delincuencia menor, pequeños hurtos, vandalismo), no resultando eficaz para la prevención de delitos violentos.

Ahora bien, ante la efectiva contribución al delito por parte de potenciales víctimas que carecen no ya de sistema de seguridad eficaces, sino de una mera contraseña o clave personal que, de alguna forma, disuada a cualquier sujeto de acceder a su sistema operativo, las medidas derivadas de la teoría de la prevención situacional se presentan como una alternativa efectiva para prevenir la delincuencia cibernética, puesto que inciden en la modificación del comportamiento de la víctima y, consiguen, por ende, una reducción de los riesgos derivados de las oportunidades espaciales de no adoptar simples medidas preventivas ligadas a la seguridad informática.

Alta cifra negra e impunidad.

Una de las principales características de los delitos informáticos es su elevado nivel de tecnicidad con una clara incidencia en el ámbito probatorio, hecho éste que provoca una alta probabilidad de impunidad que, a su vez, también se vincula a la elevada "cifra negra" existente frente a esta clase de criminalidad.

Lejos de entrar, sin embargo, en cuestiones relacionadas con la tecnicidad de estos comportamientos, que excederían los límites de este trabajo, vamos a centrar la atención en la impunidad derivada de la conocida como "cifra negra" y el papel de las víctimas en la misma. Tal y como se acaba de poner de manifiesto, la contribución de la víctima a la comisión del delito cibernético es determinante en numerosas ocasiones para entender la elevada tasa de criminalidad, pero también la alta cifra negra, al no reconocer su condición de víctima, no presentar denuncias o no continuar hasta el final

sus pretensiones procesales.

Por lo que respecta a los supuestos en los que las víctimas desconocen su condición de tal, éstos se explican como consecuencia de las dificultades de naturaleza técnica existentes. El sistema de trabajo a tiempo real, que permite el tratamiento instantáneo de los datos o las modificaciones de los programas, o la copia de unos y de otros, por lo general, sin dejar huella de las operaciones realizadas, favorece un fenómeno criminógeno en el que la víctima desconoce la lesión sufrida o, en última instancia, toma constancia de dicho hecho transcurrido cierto tiempo, desde la comisión del mismo. Son los supuestos de ataques dirigidos contra personas naturales, en los que la cifra negra se relaciona con la llamada "invisibilidad del delito informático". Esta invisibilidad tendría su razón de ser en la relatividad del espacio y tiempo, anteriormente mencionada, a través de la cual el delincuente se inviste con los más absolutos atributos de intemporalidad y ubicuidad. Este carácter anónimo provoca en la víctima la sensación de que la justicia penal no podrá dar con el responsable y siente que se enfrenta a un ser invisible frente a cuyos ataques sólo queda resignarse, por lo que pocas veces denuncian los hechos que se dan en su perjuicio.

Cuando los ataques delictivo-informáticos son dirigidos contra empresas o corporaciones, la "cifra negra" de criminalidad encuentra su razón de ser en la "publicidad negativa" que ello significa para las propias empresas atacadas. Los incidentes en Internet suelen ser asociados con el nivel de seguridad informática que poseen las empresas o corporaciones atacadas. Ello genera, como es evidente, desprestigio en la empresa atacada, descrédito de la fiabilidad de la gestión de la propia empresa y, en diversas ocasiones, temor a que como consecuencia de las investigaciones policiales se lleguen a desvelar estrategias o secretos comerciales, industriales o científicos. Por esa razón un alto número de incidentes de seguridad en Internet son mantenidos en reserva por decisión de las propias víctimas.

En general, bien sea por el desconocimiento de la intromisión ilegítima, bien por el desprestigio que conlleva la denuncia de un ataque informático, la realidad de la "cifra negra" en el ámbito de la cibercriminalidad se hace más patente que en otra clase de proceso criminógeno y genera inevitablemente un sentimiento de impunidad a la hora de afrontar al comisión de estos delitos, a pesar de las ventajas de la

presentación de denuncias.

Tal y como se ha puesto de manifiesto, el papel que ocupa la víctima en el progreso de este proceso criminal no favorece la reducción de la cifra negra. Las oportunidades de las que disponen los potenciales autores, frente a colectivos de víctimas que carecen de medidas preventivas eficaces, llegando, incluso, en ocasiones, a no percibir su condición de tal, se presenta como otro elemento adicional que incide nuevamente en la impunidad de estas conductas, al favorecer la invisibilidad de los comportamientos cibernéticos. Con todo, en el sentido manifestado, la reducción, tanto del papel de la víctima, en la comisión de la cibercriminalidad, como de la elevada tasa de cifra negra, se convierten, desde una perspectiva victimológica, en el objetivo fundamental a tener en cuenta, como primeros factores para la erradicación y sanción de estas conductas. En efecto, sólo la adopción de estrategias preventivas de incremento del riesgo y del esfuerzo para cometer el delito se presentan como instrumentos eficaces en la lucha contra la cibercriminalidad. Si a ello se añade la presentación sistemática de denuncias se conseguirá aminorar la invisibilidad de muchas de estas conductas, cuya esencia, junto a la complejidad técnica de los procesos en los que se ubican, reside igualmente en el desconocimiento de las mismas por parte de la propia Administración de Justicia.

Impacto, extensión y posibilidades de reparación

En el caso de delitos contra la propia imagen y contra la dignidad o en el caso de la difusión de imágenes de otro tipo de delitos, el ciberespacio proporciona una extensión ilimitada de la victimización, en el sentido de que inmediatamente, y de forma quizá permanente en cuanto que alguien se haya podido descargar las imágenes[1], esas imágenes y/o datos son accesibles de forma global para todos los posibles usuarios de Internet a escala global independientemente de dónde se encuentren.

[1] Fuera del supuesto de las descargas privadas y, más allá del ámbito penal, se encuentra el derecho al olvido como límite a la perennidad digital, reconocido recientemente, respecto de los buscadores, por la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 (Mieres 2014).

Por tanto, resulta vital trabajar con los sentimientos de vergüenza y humillación de las víctimas directas e indirectas, así como incentivar formas de reparación a través del espacio virtual.

En el caso concreto del fraude en Internet, en el estudio del Instituto Internacional de Victimología de Tilburg (INTERVICT), se recurrió a la metodología de los grupos focales o de discusión (focus group), revelándose como un método adecuado para recabar información real sobre las experiencias de victimización y de las necesidades de las víctimas. Una característica común es que los relatos de victimización incluían la victimización primaria y secundaria. Respecto de esta última: "En el caso de las víctimas de fraude, un impedimento específico para un tratamiento de apoyo adecuado puede ser el hecho de que la policía encargada de la denuncia de este tipo de delitos no vea ninguna perspectiva de éxito en la investigación, o incluso pueden llegar a dudar de que haya existido un delito". Asimismo se subraya que es erróneo que el impacto victimal en fraude por Internet se restringe al daño económico (van Dijk 2014, 209-211).