

MIEDO AL DELITO EN CONTEXTOS DIGITALES: UN ESTUDIO CON POBLACIÓN URBANA¹

César SAN JUAN, Laura VOZMEDIANO² y Anabel VERGARA

*Instituto Vasco de Criminología
Universidad del País Vasco*

“Pensando con sana utopía hablaríamos de criminalidad más que de delito. Criminalidad que no es la suma de los delitos, sino algo distinto: como el océano no es la suma de las gotas de agua [...]. El delito necesita una remodelación que lo patencie como obra no solo del delincuente sino también como obra de construcción social en la que interferimos el legislador, los controles formales e informales, las víctimas y no menos los denunciantes”. Antonio Beristain³

INTRODUCCIÓN

El miedo al delito y la percepción de inseguridad son, en la actualidad, temas de interés para la investigación científica, pero también para los medios de comunicación, los ciudadanos mismos y las instituciones implicadas en la toma de decisiones para la promoción de la calidad de vida urbana. Y es que un aspecto que todo investigador en ciencias sociales debe tomar en consideración es la relevancia social de la temática de su investigación. En este caso, la relevancia del estudio del miedo al delito viene dada, principalmente, por los efectos que tanto para los individuos, como para la comunidad, puede tener una situación generalizada de miedo a ser víctima de delitos. Efectos que, como veremos, pueden ser independientes de la situación objetiva de riesgo, es decir, de la tasa de delitos que una zona o ciudad concreta soporta.

1. Este trabajo ha sido parcialmente financiado con una beca para equipos de investigación de la Escuela Vasca de Estudios Territoriales y Urbanos (Instituto Vasco de Administración Pública, Gobierno Vasco).

2. El trabajo de esta autora se ha financiado con una ayuda del Programa de Formación de Investigadores del Dpto. de Educación, Universidades e Investigación del Gobierno Vasco.

3. *Criminología, Victimología y Cárceles. Tomo I.* (1996, p. 241).

El miedo al delito –como la percepción de inseguridad en general– hace referencia a percepciones y emociones subjetivas de los ciudadanos y, por tanto, no siempre se corresponde con índices objetivos de seguridad y delincuencia. Es más, frecuentemente se ha observado que la inseguridad ciudadana objetiva y la percibida son divergentes, y que en un contexto objetivo de delitos en decrecimiento crece, por distintas razones, la percepción de inseguridad. Por ejemplo, Schweitzer, Kim y Mackin (1999) ejemplifican esta situación con el sostenimiento del miedo al delito en los EEUU en la década de los 90, mientras las tasas de delincuencia disminuían.

En la actualidad, y en nuestro contexto, puede observarse este mismo fenómeno. En la última encuesta europea de delito y seguridad (EU ICS 2005), se observa que en varios países el miedo al delito es alto, aunque el riesgo objetivo de victimación sea bajo en relación al resto de Estados considerados. Así, España, que ocupa el último lugar en cuanto a prevalencia de victimación, se sitúa en el sexto puesto en temor al delito, entre 19 Estados (Van Dijk et al., 2008). En nuestro contexto geográfico más inmediato, el País Vasco, se constata que las tasas de delincuencia son estables desde hace diez años; los debates y noticias sobre una “creciente inseguridad”, sin embargo, son continuos.

Estas consideraciones ponen de manifiesto que el miedo al delito constituye un problema –un objeto de estudio– por sí mismo, relativamente independiente del diagnóstico sobre la delincuencia objetiva, si bien esta última siempre será tenida en cuenta junto a otros elementos que definen el contexto en el que se estudia el fenómeno de interés. Así, en nuestros días una nueva dimensión espacial está surgiendo como escenario de una nueva criminalidad. Nos referimos a los contextos digitales y a la ciber-delincuencia. Según Subijana (2008), los ciber-crímenes tienen cuatro aspectos característicos:

- Se cometen fácilmente.
- Requieren escasos recursos en relación al perjuicio que causan.
- Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.
- Se benefician de las lagunas de punibilidad que pueden existir en determinados Estados, algunos de los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas.

Actualmente, el objetivo principal del ciber-delincuente parece ser fundamentalmente el lucro. Da la impresión de que se acabó la época del *hacker* en busca de prestigio, publicidad y ahora todo se reduce al beneficio económico cortoplacista por métodos ilícitos. El fraude *on-line* sigue en constante crecimiento, como así alertan los expertos. Uno de los factores que sin duda incrementará la proliferación de nuevas formas de fraude *on-line* es la situación de crisis económica en la que se encuentra España particularmente que será aprovechado por los delincuentes potenciales para conseguir elevar el número de víctimas. Según un informe de la empresa S21sec⁴, el hecho de engañar a usuarios mediante falsas promesas de trabajo, loterías, premios

4. Fuente: <http://www.s21sec.com/descargas/Informe%20fraude%20Online%202007-2008.pdf>

y en general cualquier argumento que pueda suponer un ingreso de dinero fácil se seguirá produciendo de manera cada vez más acentuada durante este año 2009 y siguientes, optimizando progresivamente las técnicas utilizadas hasta llegar a un grado de sofisticación que supondrá un aumento en el número de ataques “personalizados” orientados hacia diferentes perfiles de usuario. Hasta el punto, se asegura en este informe, de lograr cierta individualización en los mensajes destinados a captar la atención de los usuarios. Esta tendencia se verá facilitada en gran medida por la proliferación del uso de redes sociales y por el aprovechamiento por parte de los atacantes de todas aquellas fuentes que puedan contener información que facilite el proceso de ganarse la confianza de la víctima.

Por otra parte, los troyanos, programas informáticos maliciosos que pueden robar contraseñas, están ganado terreno a la técnica del *phising* (envío masivo de correos electrónicos falsos para lograr claves bancarias) que cada vez atienden menos internautas que han mejorado en los últimos años su nivel de información. Según los datos del Instituto Nacional de Tecnologías de la Comunicación⁵, en 2007, el 70% de los ataques con fines económicos fue con la técnica del *phising*, mientras que el 30% restante vino a través de troyanos. Este porcentaje varió en 2008 (60% frente a 40%) y es previsible que se iguale o cambie este año en el que ha irrumpido el gusano Downadup que ha infectado a más de 9 millones de ordenadores por una vulnerabilidad del sistema operativo y que es capaz de transmitirse a través de dispositivos USB. Las estafas cometidas a través de Internet y el intercambio de archivos de pornografía infantil a través de la red fueron los delitos informáticos más habituales detectados por la Fiscalía en Gipuzkoa durante el año 2008. Ésta es una de las conclusiones principales recogidas en la Memoria realizada por el Ministerio Público sobre los delitos cometidos en esta provincia durante el año pasado. El documento, que por primera vez analiza la delincuencia informática al contar desde 2008 con un fiscal especializado en este tipo de criminalidad, explica que durante el año pasado se incoaron un total de 59 procedimientos, 38 de los cuales se encontraban en investigación a finales de año, mientras que en 14 casos se formuló acusación contra los imputados y siete más fueron archivados. El escrito constata “un predominio de las denuncias por estafa (30), seguidas por los delitos de pornografía infantil (14) y, a cierta distancia, los cometidos contra la libertad como las amenazas y las coacciones (3) y contra el honor (2)”. En la Memoria, la Fiscalía alerta además de la “preocupante” aparición del delito de “espionaje industrial” relacionado con la delincuencia informática, “por cuanto que la especial pujanza de la industria de la máquina-herramienta de alta tecnología” en Gipuzkoa constituye “el caldo de cultivo idóneo para este tipo de conductas”. “La copia inadvertida de datos empresariales sensibles, o bien su destrucción, son fenómenos que pueden suponer pérdidas de más de un millón de euros en un solo acto ilícito”. La Fiscalía alerta además sobre la proliferación de delitos informáticos como la “usurpación” de la personalidad de la víctima para contratar servicios telemáticos por Internet o para utilizarla ilegalmente en la red a raíz de “conflictos personales derivados de relaciones sentimentales”. En este punto, advierte de la “preocupante importancia” que están cobrando las “coacciones y amenazas asociadas a la revelación de secretos personales” en Internet, que son “frecuentemente cometidas por ex parejas

5. Fuente: <http://www.inteco.es/>

y menores” que utilizan de forma “ilegítima” las “claves personales” de la víctima para acceder a su correo electrónico. De esta forma, los delincuentes remiten “una serie de mensajes injuriosos” desde el correo de los perjudicados a su lista de contactos con los que pretenden desacreditarlos ante “su círculo de amistades”, llegando en algunos casos incluso a revelar su orientación sexual. La Fiscalía cita asimismo delitos como las estafas que se producen mediante la venta falsa de objetos en portales de subastas o las que se comenten engañando a las víctimas para que proporcionen a los delincuentes sus claves bancarias de internet para luego sustraerles dinero de sus cuentas. En ocasiones, los delincuentes, radicados en el extranjero, utilizan intermediarios en cuyas cuentas ingresan las transferencias delictivas para que éstos las cobren y se las reenvíen por mensajería a cambio de una comisión.

En este sentido podríamos decir que existe una amenaza potencial generalizada en los contextos digitales. La última encuesta del Instituto Nacional de Tecnologías de la Comunicación (INTECO) apunta que el 72% de los hogares españoles tiene algún tipo de código malicioso. El 95% de los encuestados por INTECO⁶ declaraba tener un antivirus, mientras que sólo el 87 % de ellos lo tenía realmente. Así, el 76% dice utilizar cortafuegos, el 69% bloqueo de páginas y el 56% sistemas *anti-spam*. Los porcentajes descienden al 34% en el caso de copias de seguridad, partición del disco duro, etc. Por otro lado las pymes no consideran los Sistemas de Gestión de la Seguridad de la Información como una inversión necesaria y su dificultad técnica muchas veces les supera. El problema es que incluso muchos de estos esfuerzos son en gran parte inútiles porque los *botnets* que distribuyen malware como los gusanos son todavía relativamente indetectables por los programas antivirus que se comercializan.

En definitiva, la hipótesis que queremos poner en evidencia en esta investigación es el desfase actualmente existente entre la amenaza a la que están expuestos los usuarios de Internet y la percepción de inseguridad que suscita esa amenaza, con el consiguiente riesgo que puede conllevar. En todo caso, parece claro que la probabilidad de ser víctima de un delito en contexto digital es mayor que la de ser víctima de un robo en la calle. Sin embargo, nuestra hipótesis es que la percepción de inseguridad es mayor en este último escenario. Para analizar y, en su caso, confirmar este planteamiento realizamos un estudio con una muestra representativa de ciudadanos y ciudadanas de la ciudad de Bilbao que se presenta a continuación.

MÉTODO

Muestra

La muestra está compuesta por 1700 residentes en la ciudad de Bilbao, mayores de edad. Se realizó un muestreo probabilístico y estratificado por distrito, género y edad. Respecto a la estratificación por distrito de residencia (asumiendo los ocho distritos administrativos en los que se divide la ciudad), el número de entrevistados en

6. Fuente: <http://www.inteco.es/>

cada distrito fue proporcional a su población. En lo que se refiere al género, se estableció una distribución equitativa y, finalmente respecto a la edad, se fijaron cuotas para asegurar la adecuada representación de todos los segmentos de edad en la muestra. Siendo la población objeto de estudio el total de ciudadanos residentes en Bilbao, con una muestra de 1.700 entrevistados y, establecido el nivel de confianza al 95%, el error muestral queda limitado al $\pm 2,4\%$.

Como resultado de los criterios establecidos, la muestra está equilibrada al 50% respecto al género. La edad de los entrevistados oscila entre los 18 y 95 años, siendo la media de 47 y la desviación típica de 15. El porcentaje de sujetos que pertenece a los grupos de edad establecidos por los investigadores, así como otros indicadores socio-económicos recogidos, se indica en la Tabla 1, que presenta un resumen de las características de la muestra.

Es reseñable que se ha procurado, y a juicio de los autores conseguido, una heterogeneidad notable en las distintas variables socio-demográficas lo que, combinado con el importante tamaño muestral, nos permite tanto generalizar los resultados al conjunto de los residentes de la ciudad como focalizar el estudio de algunas cuestiones concretas en grupos determinados: por ejemplo, los mayores, las mujeres o los jóvenes.

Como se detalla en el apartado de resultados de esta muestra representativa el 53% de los sujetos (N= 902) dice ser usuaria de Internet.

Materiales

Se empleó un instrumento diseñado *ad hoc* por el equipo investigador. La fiabilidad y validez de la primera versión del instrumento fue contrastada por medio de un estudio piloto, que constituyó una de las primeras tareas abordadas por el equipo investigador en este proyecto. Dicho estudio piloto contó con una muestra de 60 sujetos, pertenecientes a tres distritos con tipología socioeconómica alta, media y baja (Abando, Deusto y Recalde), y las cuotas de género y edad fijadas fueron similares a ya descritas para la muestra final de este estudio. Los resultados de los análisis con el estudio piloto, ratificaron la adecuada fiabilidad y validez de la escala.

Variables incluidas en el instrumento

- *Variables socio-demográficas.* Ubicadas al principio y final del cuestionario, se incluyeron cuestiones para medir el género, la edad, residencia, número de hijos, nivel de estudios, poder adquisitivo, actividad que desempeña, etc.
- *Miedo al delito* en escenario urbano y miedo al delito en contexto digital.
- *Medidas de autoprotección* o evitación de riesgo percibido.

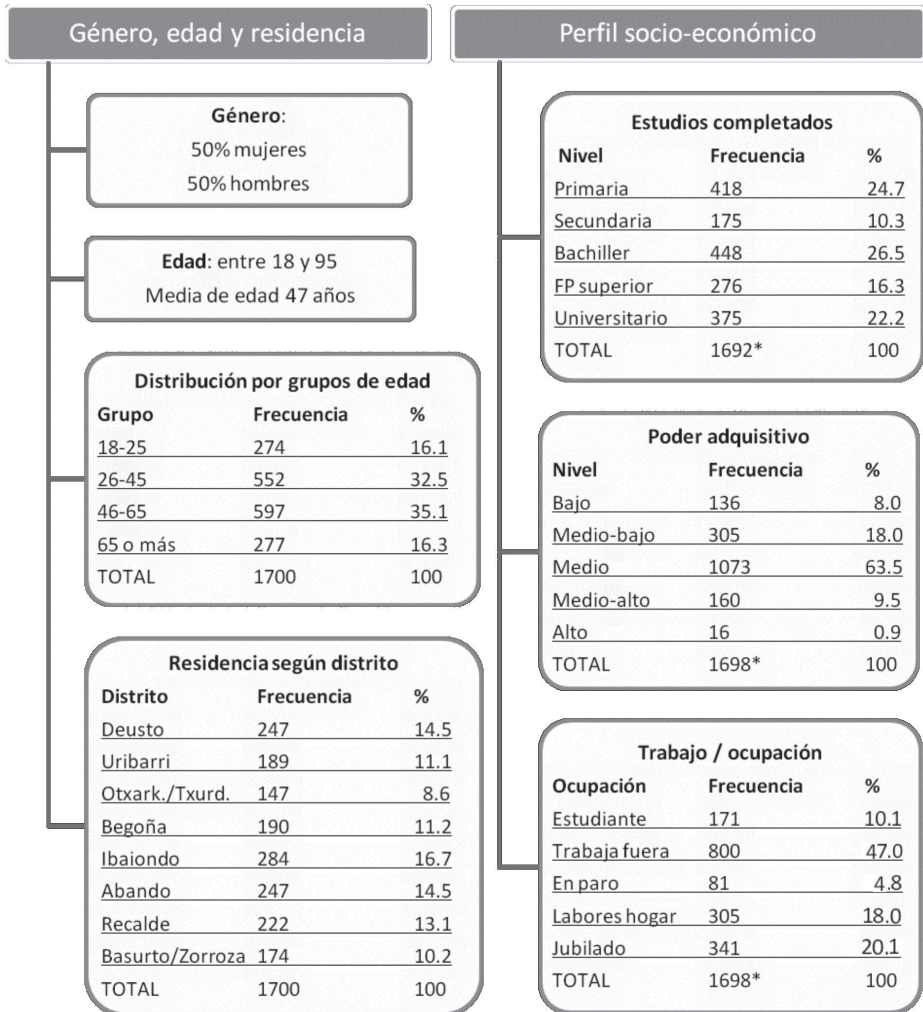


Tabla 1. Resumen de datos socio-demográficos que caracterizan la muestra.

* Totales menores que 1700, ya que algunos sujetos prefirieron no aportar ese dato.

PROCEDIMIENTO

Primeramente, se formó a los encuestadores en la selección de sujetos para completar las cuotas establecidas según el muestreo y en la aplicación del cuestionario. Estas personas recogieron los datos mediante entrevista telefónica, siguiendo las pautas recibidas en la fase de formación, así como las indicaciones que, por escrito, constaban en cada ejemplar del cuestionario. Así, se telefoneó a los hogares que

eran seleccionados al azar en las unidades geográficas determinadas (distritos), comprobando para cada sujeto que aceptaba colaborar en el estudio, que residiera en el distrito de interés, fuera mayor de edad y su género y edad se correspondieran con las necesidades de la fase concreta de la recogida de datos. Realizadas estas comprobaciones, se procedía a entrevistar al sujeto. A todos los entrevistados se les ofreció la posibilidad de comprobar la identidad del entrevistador, así como la veracidad de los datos ofrecidos respecto a la entidad responsable del estudio y sus objetivos. Sólo si el cuestionario era respondido hasta el final, y el número de ítems no contestados se mantenía por debajo de un límite preestablecido, pasaría a formar parte de la base de datos del estudio. Una vez completados los 1700 cuestionarios que, cumpliendo las condiciones citadas, constituyeron la muestra del estudio, éstos fueron remitidos por la empresa encargada de las entrevistas telefónicas al equipo investigador. Los cuestionarios completados, por tanto, se almacenaron en el Instituto Vasco de Criminología, centro de trabajo del equipo investigador, donde permanecen fuera del alcance de terceras personas para garantizar su confidencialidad en todo momento. Las respuestas fueron codificadas en una base de datos para realizar los análisis estadísticos correspondientes con el software SPSS 15. Los resultados de estos análisis se presentan en el siguiente apartado.

RESULTADOS

De las 1700 personas participantes en este estudio, un total de 902 dicen ser usuarias de Internet. Como se puede observar en la Tabla 2, un 12,4% lo usaría ocasionalmente y un 40,7% del total de la muestra dice usarlo habitualmente. Así, en el contexto urbano objeto de esta investigación podríamos establecer que casi la mitad de la población (46,9%) no usa Internet jamás.

Uso Internet	Frecuencia	Porcentaje
Nunca	798	46,9%
Ocasionalmente	210	12,4%
Habitualmente	692	40,7%
Total	1.700	100%

Tabla 2. Usuarios de Internet.

Dicho esto, nos interesó especialmente analizar las diferencias socio-demográficas entre usuarios y no-usuarios de Internet encontrando algunos datos destacables que se detallan en la Tabla 3 (N= 1700).

VARIABLES	GRUPOS	N	Media
Edad	No Usuarios	791	56,87
	Internautas	901	38,70
Probabilidad de ser víctima	No Usuarios	680	3,20
	Internautas	815	3,67
Nivel de estudios	No Usuarios	790	1,26
	Internautas	902	2,66
Poder adquisitivo	No Usuarios	796	1,63
	Internautas	894	1,89

Tabla 3. Diferencias entre Internautas y no-usuarios de Internet

Como se puede apreciar en la Tabla 3 los Internautas son significativamente más jóvenes ($p = .000$; $F = 592,2$), con un nivel de estudios superior ($p = .000$; $F = 495,17$) y mayor poder adquisitivo auto-reportado ($p = .000$; $F = 50,38$) que los no-usuarios de Internet. Por otra parte, también hemos detectado que los Internautas tienen mayor temor a ser víctimas de un delito (en contexto no-digital) que los no-usuarios de Internet ($p = .000$; $F = 13,99$).

En los análisis que se presentan a continuación vamos a centrarnos en la submuestra de usuarios de Internet ($N = 902$), focalizando nuestra atención en tres tipos de perfiles de usuarios diferentes. Vamos a distinguir entre grupo a) el grupo de Internautas que exclusivamente usan banca *on line* ($N = 132$); grupo b) el grupo de Internautas que exclusivamente realizan compras por Internet ($N = 112$) y grupo c) el grupo de Internautas que hemos denominado multi-usuarios y realizan ambas conductas: uso de banca *on line* y compras por Internet ($N = 271$).

Las variables que hemos considerado para definir los perfiles son, por un lado, el miedo a ser víctima de un delito en contexto real (miedo a que te roben en la calle y miedo a que te roben en tu vehículo) y, por otro, miedo a ser víctima de un delito en contexto digital (miedo a ser víctima de delito usando banca *on line* o comprando en Internet). También hemos medido dos variables adicionales relacionadas con las medidas de autoprotección. Por un lado, la aplicación de medidas de seguridad en contexto real que hemos etiquetado como “*autoprotección real*” (evitar zonas urbanas por considerarlas inseguras) y, por otro, los recursos y conocimientos auto-reportados para evitar ser víctima de un delito en contexto digital y que hemos etiquetado como “*autoprotección digital*”.

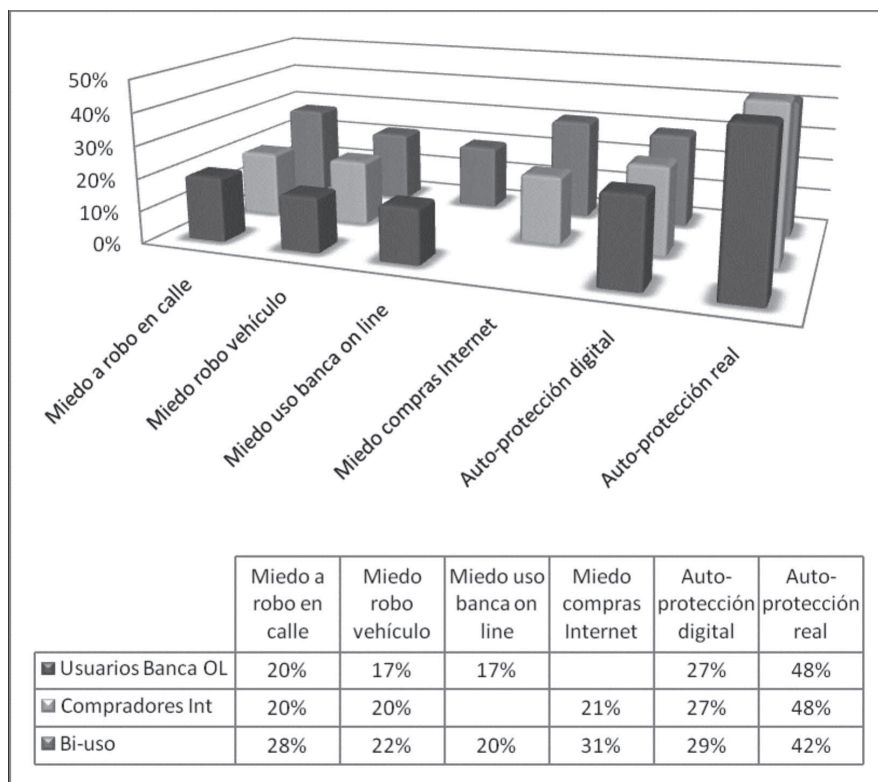


Tabla 4. Perfiles de uso de Internet, percepción de inseguridad y medidas de protección.

Como podemos observar en la Tabla 4 no existen apenas diferencias en el perfil de usuarios de banca *on line* y compradores por Internet. Es en torno al 20% de cada uno de los dos grupos que han tenido miedo a que les roben en la calle o, en el caso del grupo *b*, haciendo compras por Internet. Si acaso es algo menor el porcentaje de sujetos (17%) en el grupo de usuarios de banca *on line* que dice tener miedo a que les roben en el coche o en contexto digital. En todo caso, no podríamos decir que exista una mayoría de personas que experimenta un mayor temor en un contexto que en otro.

El perfil del grupo que hemos denominado multi-usuarios sí ofrece un cierto distanciamiento con respecto a los anteriores. En general encontramos un mayor porcentaje de sujetos que han tenido miedo en contexto real que llega al 28% en el caso del temor a que te roben en la calle. También identificamos un porcentaje de sujetos que tienen miedo a ser víctimas de un delito usando la banca *on line* (20%) superior al grupo que usa solo Internet con este fin (17%), siendo especialmente destacable el porcentaje de sujetos que tiene miedo a ser víctima de un delito comprando en Internet (31%). Parece existir una mayor conciencia de vulnerabilidad en este tercer grupo. En todo caso, en los tres grupos es netamente superior el porcentaje de sujetos que toma

medidas de autoprotección en contexto real (el 48% en los *grupos a y b*) en contraposición al porcentaje de sujetos que toma medidas en contexto digital (27% en los *grupos a y b*, y 29% en el *grupo c*). El objetivo de este estudio, que no es otro que poner en evidencia la paradoja existente entre la probabilidad de ser víctima de un delito en un contexto digital y adoptar medidas de autoprotección parece ponerse de manifiesto en las frecuencias observables en la tabla 4. Efectivamente, siendo más probable ser víctima de un robo o estafa en Internet que el hecho de ser víctima de un robo en la calle, sin embargo es muy superior el porcentaje de sujetos que adoptan medidas para evitar este extremo.

En este sentido pueden ser relevantes las tablas de contingencia presentadas a continuación correspondientes a los usuarios de banca *on line* y a los compradores por Internet respectivamente (Tablas 5 y 6). Efectivamente, en ellas podemos observar que casi un 70% de los individuos que han tenido miedo alguna vez a que les roben en la calle nunca lo han experimentado usando la banca *on line*. Por su parte, en torno al 59% de personas compradoras en Internet que han tenido miedo alguna vez a que les roben en la calle nunca han temido ser víctimas de un delito en contexto digital.

			Miedo usando banca online		Total
			No	Sí	
Miedo a robo en la calle	No	Recuento	256	45	301
		% de Miedo a robo en la calle	85,0%	15,0%	100%
	Sí	Recuento	71	32	103
		% de Miedo a robo en la calle	68,9%	31,1%	100%
	Total	Recuento	327	77	404
		% de Miedo a robo en la calle	80,9%	19,1%	100%
			Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson			12,923(b)	1	,000

Tabla 5: de contingencia Miedo a robo en la calle * Miedo usando banca online

			Miedo haciendo compras por Internet		Total
			No	Sí	
Miedo a robo en la calle	No	Recuento	211	66	277
		% de Miedo a robo en la calle	76,2%	23,8%	100,0%
	Sí	Recuento	58	41	99
		% de Miedo a robo en la calle	58,6%	41,4%	100,0%
	Total	Recuento	269	107	376
		% de Miedo a robo en la calle	71,5%	28,5%	100,0%
			Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson			11,081(b)	1	,001

Tabla 6: de contingencia Miedo a robo en la calle * Miedo haciendo compras por Internet

DISCUSIÓN

En definitiva, lo que hemos querido poner en evidencia es la existencia de una mayor tendencia a la percepción de invulnerabilidad en contextos digitales con respecto al miedo percibido en espacios urbanos. Sería una suerte de sentimiento paradójico, y nada adaptativo, toda vez que existe una menor percepción de riesgo en aquel contexto donde existe, según todos los estudios, una amenaza objetiva mayor.

El miedo al delito es objeto de investigación en las ciencias sociales desde los años sesenta, habiendo generado un gran volumen de investigación en disciplinas tales como la sociología, psicología, geografía humana... Pero muy especialmente, se trata de un campo de trabajo que atañe a la criminología y que ha recibido considerable atención por especialistas de esta disciplina así como generado un gran volumen de publicaciones. Para una visión general de las publicaciones en este campo, pueden consultarse revisiones de la literatura (Hale, 1996; Van Beek, 2004); también puede consultarse la compilación de artículos del volumen editado por Ditton y Farrall (2000).

No sólo la investigación científica se ha interesado por el miedo al delito; paralelamente, y especialmente en algunos países anglosajones, la reducción del miedo al delito se ha convertido en objetivo de las políticas institucionales y de la práctica policial. Por ejemplo, en la información que ofrece a la ciudadanía en su página web el Home Office, en Reino Unido, podemos encontrar la declaración siguiente: *“The risk of becoming a victim of crime has fallen sharply in recent years. [...] But we aim to reduce this level even further. And to reduce fear of crime, which has risen even as the number of crimes actually committed has fallen. We believe everybody has the*

right to feel safe as they go about their daily lives.”⁷. En estas afirmaciones se pone de manifiesto que la reducción del miedo al delito es un objetivo en sí mismo, asumido por las autoridades y la policía, para proteger ese derecho a que los ciudadanos se sientan seguros en los espacios en que se desarrolla su vida diaria. El objetivo último es similar a lo que se ha denominado “democratización del espacio urbano” (San Juan y Vozmediano, 2009), abogando por el diseño de espacios públicos que sean percibidos como seguros por todos los ciudadanos.

En este punto, y tras décadas de estudio del miedo al delito, encontramos que actualmente la ciudad ya no es el único escenario en que el ciudadano puede experimentar temor ante la supuesta amenaza del delito, adaptando su conducta a unas percepciones de riesgo, muchas veces poco ajustadas a la realidad. Un nuevo escenario puede plantearnos una problemática muy similar; y no es otro que Internet. Lo que se ha denominado ciber-delito, o delitos cometidos a través de internet, es una amenaza real para un número cada vez mayor de ciudadanos. La comunidad internauta crece día a día, con casi 1.600 millones de usuarios en todo el mundo⁸. De modo paralelo, crecen los delitos cometidos a través de Internet y el número de víctimas de estos delitos: en Estados Unidos, el IC3 (Internet Crime Complaint Center⁹) centro que recoge denuncias de ciudadanos que han sido víctimas de un ciber-delito, plantea en su último informe sobre delito en Internet (IC3, 2008) que ese año establece un record en el número de denuncias. Como muestra la Tabla 7, las denuncias se han multiplicado por diecisiete desde el año 2000.

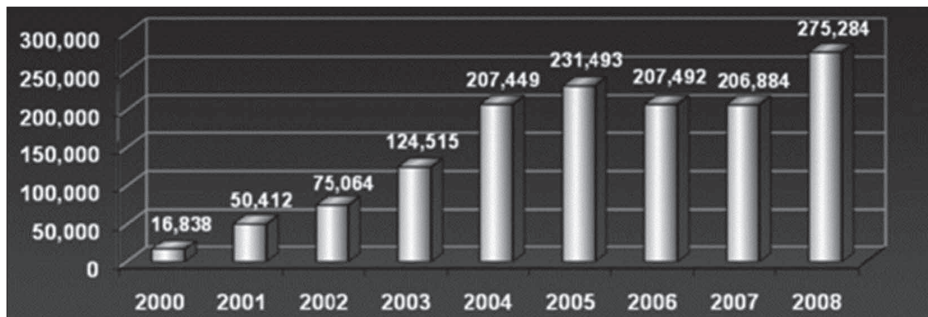


Tabla 7. Número de denuncias de ciber-delitos en el Internet Crime Complaint Center, en función del año en que fueron presentadas.

Fuente: 2008 Internet Crime Report (IC3).

7. “El riesgo de ser víctima de un delito se ha reducido drásticamente en los últimos años. [...] Pero nuestro objetivo es reducirlo aún más. También reducir el miedo al delito, que ha aumentado incluso cuando el número de delitos efectivamente cometidos ha disminuido. Creemos que todo el mundo tiene derecho a sentirse seguro en su vida diaria”. Traducción propia. Texto original disponible en: <http://www.homeoffice.gov.uk/crime-victims/reducing-crime>.

8. 1.596.270.108 usuarios de Internet en todo el mundo, a 31 de marzo de 2009, según www.internetworldstats.com.

9. <http://www.ic3.gov>.

Con el progresivo crecimiento de la comunidad de internautas y, paralelamente, de los ciber-delitos, crece también el interés de los investigadores, que en los últimos años se interesan cada vez más por la delincuencia en Internet y sus víctimas. Una búsqueda en la base de datos del *ISI Web of Knowledge* con las palabras clave “*Internet and crime*” arroja 117 resultados –hasta el año 2008– en las categorías de Criminología y Penología, Psicología y Ciencias de la conducta, Informática y Sociología. Si analizamos los resultados por año de publicación, encontramos que hay un interés creciente en el tema, que se refleja en un mayor número de publicaciones en los años más recientes, como muestra la Tabla 8; pero todavía con un escaso volumen de trabajos, si comparamos el ciber-delito con el delito *tradicional*. Hay todavía mucha labor de investigación a desarrollar para conocer los perfiles de delincuente y víctima en este nuevo contexto, así como las características de los *nuevos delitos* cometidos en Internet. Búsquedas similares pero en castellano, en las bases de datos Dialnet e ISOC (CSIC) arrojan sólo una veintena de resultados.

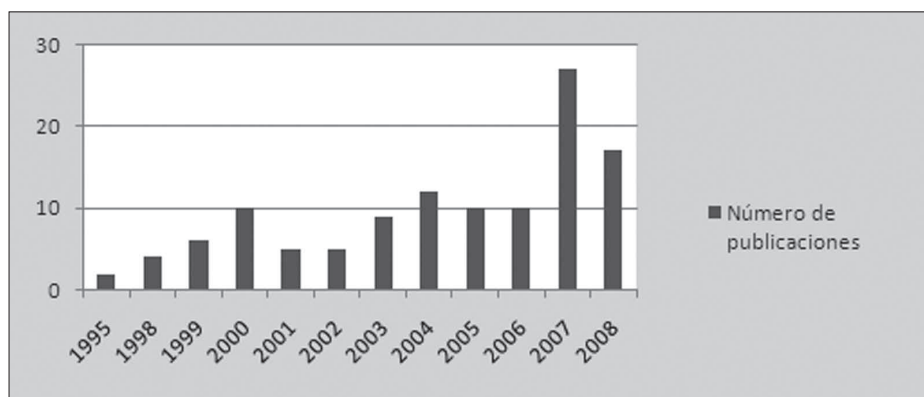


Tabla 8. Número de publicaciones con los topic “*Internet and Crime*” en el *ISI Web of Knowledge*, según el año.

Elaboración propia con los datos del ISI Web of Knowledge.

Si en el estudio de los ciber-delitos todavía quedan muchas cuestiones por abordar, el miedo a los ciber-delitos ha recibido todavía menor atención, y son escasos los trabajos al respecto. Sin embargo, el miedo a sufrir un delito en Internet presenta notables paralelismos con el temor a delitos en espacios urbanos, que sugieren que su investigación puede ser relevante. En ambos casos se trata de escenarios que ofrecen gran cantidad de estímulos al sujeto, que debe seleccionar aquellos estímulos a los que prestar atención al categorizarlos como relevantes; en ambos casos, a menudo la información sobre los riesgos de ser víctima de un delito es limitada o errónea, por lo que las percepciones de riesgo pueden estar muy alejadas de la realidad; y si un alto temor al delito en la vida real pueden inhibir ciertas conductas, es esperable que el temor a sufrir un delito en Internet pueda inhibir su uso, o ciertas conductas *on-line* (compras, uso de banca *on-line*, etc.). A pesar de ello, pocos investigadores se han ocupado del estudio científico del temor a los ciber-delitos. Sí se han realizado trabajos sobre las estimaciones de riesgo de ser víctimas de un delito al realizar compras por Internet, que

principalmente han visto la luz en revistas de comunicaciones y tecnologías de la información. Trabajos similares, orientados a cuantificar los efectos de las percepciones de los usuarios en los negocios realizados a través de Internet, han sido llevados a cabo por parte de empresas consultoras o bien por empresas que trabajan directamente en la venta *on-line*. Los resultados de estos trabajos se divulgan principalmente en prensa o portales especializados, pero a menudo no es posible acceder al trabajo completo para conocer los detalles del estudio, como podríamos hacer en una publicación científica. Por ejemplo, según un portal especializado, una encuesta realizada en 2009 por la empresa consultora Gartner Inc. mostró que el 39% de los encuestados ha cambiado su comportamiento en Internet por temor a que sus datos personales sean robados y muchos de ellos estarían reduciendo el número de compras *on-line* realizadas¹⁰. Siendo escasos los trabajos recogidos en publicaciones científicas sobre este objeto de estudio, la revisión realizada ha mostrado algunas publicaciones muy interesantes, como el trabajo de Reisig, Pratt, & Holtfreter (2009). Estos autores, con una muestra de 1.000 adultos residentes en el Estado de Florida (USA) encontraron que el 57,6% de los encuestados indica que es “algo probable” o “muy probable” que sufran un robo del número de tarjeta que les produzca perjuicio mientras realizan compras en Internet. Además, sus resultados mostraron una asociación entre un mayor riesgo estimado y restricciones en el uso de Internet (realizar menos compras, pasar menos tiempo conectado). Otro trabajo interesante y muy completo es la monografía de Alshalan (2009). Este autor analizó los datos de la primera encuesta realizada en USA a nivel nacional sobre víctimas de ciber-delitos, y encontró que el 70% y el 80% de los encuestados estaba “algo preocupado” o “muy preocupado” por convertirse en víctima de alguno de los ciber-delitos que presenta (resultar su equipo *hacked*, robo del número de tarjeta al introducirlo en Internet, ser víctima de un delito relacionado con los ordenadores en general). Este temor a ciber-delitos, según dicho estudio, era mayor entre quienes habían sufrido previamente algún ciber-delito y entre quienes creían que los ciber-delitos son crímenes serios. Además, era más alto entre las mujeres, a pesar de que éstas son menos victimizadas, replicando el resultado clásico en la literatura de miedo al delito. El autor plantea que es necesario, en la investigación futura, que se estudie el efecto que estos temores pueden tener en las conductas de uso de Internet. En nuestro país, hasta donde conocemos, no se han realizado publicaciones científicas sobre el miedo al delito en contextos digitales. La prensa se ha hecho eco de algunas encuestas que se interesan por la confianza de los usuarios respecto a su seguridad personal al usar Internet, como la llevada a cabo por la empresa TNS en 16 países¹¹, que concluye que casi la mitad de los usuarios desconfía de la seguridad de su información personal cuando navega por Internet. Los usuarios de nuestro país estarían entre los más desconfiados lo que resultaría algo contradictorio con los resultados de nuestra investigación. Sin embargo, desconocemos si esta posible desconfianza se traduce en temor al delito al usar Internet y si la desconfianza o el temor influyen en las conductas de usuarios. En este escenario en que el miedo a la ciber-delincuencia ha sido todavía poco tratada en la investigación, especialmente en nuestro país, este trabajo ha tenido como objetivo llevar a cabo una primera aproximación al estudio de este fenómeno en

10. Fuente: <http://www.internetretailer.com/dailyNews.asp?id=29665>.

11. Fuente: Diarivasco.com, noticia publicada el 24.02.2009: <http://www.diarivasco.com/20090224/al-dia-sociedad/mitad-espanoles-crea-datos-20090224.html>.

nuestro contexto. En el marco de un estudio sobre seguridad subjetiva más amplio, se ha identificado a los usuarios de Internet, que respondieron a cuestiones sobre su uso de la red, y sobre su posible temor a ciber-delitos al utilizarla. Se trata de un estudio exploratorio, cuyo principal objetivo es provocar líneas de estudios posteriores más completos.

Así, por nuestra parte, hemos podido comprobar que un porcentaje significativo de sujetos que ha tenido miedo a ser víctima de un delito en la calle, jamás lo ha tenido en contextos digitales haciendo operaciones sensibles como pueden ser movimientos de dinero en banca *on line* o, lo que podría conllevar más riesgos, realizar compras por Internet. Dicha actitud es estadísticamente incoherente, como lo puede ser tener más miedo a volar que a viajar en coche. Este dato es además especialmente llamativo si tenemos en cuenta los reducidos porcentajes de sujetos que creen tener información o recursos suficientes para evitar ser víctimas de delitos informáticos. En vista de la situación descrita por la literatura especializada parece oportuno proponer una medición objetiva de riesgo real del usuario de Internet que pueda resultar operativa no solamente a la comunidad científica. También la administración y la empresa privada que operan habitualmente en escenarios digitales, necesitan herramientas de predicción de riesgo. Nosotros proponemos la siguiente ecuación a expensas de su desarrollo y confirmación ulteriores.

$$\text{Riesgo} = \frac{\text{Vulnerabilidad del sistema} + \text{Exposición}}{\text{Medidas de autoprotección}} \times \text{Amenaza potencial}$$

En dicha ecuación estamos entendiendo el riesgo como la probabilidad de ser víctima de un delito informático y la amenaza potencial, la incidencia prevista de individuos con conocimientos suficientes para perpetrar acciones ilícitas y con motivación para llevarlas a cabo.

REFERENCIAS BIBLIOGRÁFICAS

- ALSHALAN, A. (2009): *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*. Saarbrücken: VDM Verlag Dr. Müller.
- HALE, C. (1996): "Fear of crime: A review of the literature". *International-Review-of-Victimology*, 4, 79-150.
- IC3 (2008): *2008 Internet Crime Report*. Tomado el 27-03-2009 de: http://www.ic3.gov/media/annualreport/2008_ic3report.pdf.
- REISIG, M.D., PRATT, T.C., & HOLTFRETER, K. (2009): Perceived Risk of Internet Theft Victimization Examining the Effects of Social Vulnerability and Financial Impulsivity. *Criminal Justice and Behavior*, 36, 369-384.
- SAN JUAN, C. & VOZMEDIANO, L. (2009): "Democratización del espacio urbano y percepción de seguridad: una propuesta de análisis". In L. R. Ruiz Rodríguez (Ed.), *Respuestas internacionales a los retos de la seguridad* (pp. 273-280). Valencia: Tirant lo Blanch.

- SCHWEITZER, J.H., KIM, J.W., & MACKIN, J.R. (1999): "The impact of the built environment on crime and fear of crime in urban neighborhoods". *Journal of Urban Technology*, 6, 59-73.
- SUBIJANA, I. (2008): "El ciberterrorismo: Una perspectiva legal y judicial". *Eguzkilore*, 22, 169-187.
- VAN BEEK, G. (2004): *Fear of crime: feeling (un)safe and (in)secure in the risk society*. Tesis doctoral. Katholieke Universiteit Leuven, Leuven. Tomado el 19-01-2009 de: http://www.statbel.fgov.be/studies/ac084_en.pdf.
- VAN DIJK, J.J.M., VAN KESTEREN, J.N., & SMIT, P. (2008): *Criminal Victimization in International Perspective. Key findings from the 2004-2005 ICVS and EU ICS*. The Hague: Boom Legal Publishers.