LA OPORTUNIDAD CRIMINAL EN EL CIBERESPACIO

Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen

Fernando Miró Llinares

Profesor Titular de Derecho Penal. Universidad Miguel Hernández de Elche

---

MIRÓ LLINARES, Fernando. La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2011, núm. 13-07, p. 07:1-07:55. Disponible en internet: http://criminet.ugr.es/recpc/13/recpc13-07.pdf
ISSN 1695-0194 [RECPC 13-07 (2011), 29 nov]

RESUMEN: El presente trabajo analiza la cibercriminalidad, la delincuencia cometida en el ciberespacio, a partir de la hipótesis de que este nuevo ámbito de intercomunicación social, distinto al espacio físico, conllevará cambios esenciales en todos los eventos que en él tengan lugar, entre ellos, el crimen. A partir de los enfoques criminológicos de la oportunidad, y con especial atención a los presupuestos de la teoría de las actividades cotidianas, se analizan los caracteres intrínsecos y extrínsecos del ciberespacio, y se plantea si el mismo supone, y en qué medida, un distinto ámbito de oportunidad criminal que requiera de una modificación esencial de las estrategias preventivas pensadas para el delito cometido en el espacio físico. Por medio de la abstracción teórica y la conexión de los elementos del crimen con las particularidades del nuevo "lugar" de comisión delictiva, pero también con el apoyo de la revisión de los estudios empíricos existentes, se definen las propiedades del nuevo ámbito de riesgo que es el ciberespacio, se anuncia el crecimiento de la cibercriminalidad paralelo al desarrollo de la vida diaria en relación con las TIC, y se sitúa en el plano central de las estrategias de prevención la conducta de la víctima, elemento explicativo del evento criminal aún más central en el ciberespacio que en el espacio físico.

PALABRAS CLAVE: Cibercrimen, TIC, Oportunidad criminal, Teoría de las actividades cotidianas, Prevención situacional, Agresor Motivado, Objetivo adecuado, Guardián Capaz, Gestor del lugar, VIVA (Valor, Inercia, Visualización y Accesibilidad), IVI (Introducción, Valor, e Interacción), Victimización.

Fecha de publicación: 29 noviembre 2011

IVI); 2.2.2.3. Guardianes capaces y gestores del lugar "ciberespacio"; 3. Conclusiones y reflexiones para el futuro; 3.1. ¿Hacia el aumento de la criminalidad en Internet? El cibercrimen y el "efecto iceberg"; 3.2. Old wine in different bottles: particularmente, el protagonismo de la víctima en el cibercrimen y su prevención; 3.3. Líneas de futuro: de las actividades cotidianas a la prevención (situacional) del cibercrimen.

1. INTRODUCCIÓN. LA CIBERCRIMINALIDAD, SU COMPRENSIÓN Y SU PREVENCIÓN: OBJETO Y OBJETIVOS DEL ESTUDIO

Los debates terminológicos no suelen deberse a meras preferencias conceptuales basadas en la estética o en la autoría del término, sino que encierran generalmente decisiones que tienen que ver con algún elemento comunicativo mejor reflejado o expresado por uno que por otro concepto. En los últimos tiempos se ha venido sustituyendo, aunque no por todos[1], la denominación de delitos informáticos por la de cibercrimen, en referencia al término anglosajón *cybercrime*[2], procedente de la unión entre el prefijo *cyber*, derivado del término *cyberspace*[3], y el término *crime*, como concepto que sirve para englobar la delincuencia relacionada con el uso de las Tecnologías de la información y la comunicación (en adelante, TIC). En los estudios criminológicos y jurídicos llevados a cabo en inglés, ya parece haberse impuesto este término frente a otros que ocupan generalmente el mismo o similar

NOTA PREVIA:
El presente artículo ha sido realizado en el marco del Proyecto de Investigación financiado por el Ministerio de Ciencia e Innovación, DER2011-26054, titulado, "Cibercriminalidad: deteccion de deficits en su prevencion juridica y determinacion de los riesgos de victimizacion para una mejor prevencion situacional criminologica".

ÍNDICE DE ABREVIATURAS UTILIZADAS:
AP, Actualidad Penal; **ACT**, Advances in Criminological Theory; **AESP,** Advances in Experimental Social Psychology; **AGUC,** Anales de Geografía de la Universidad Complutense; **APs**, American Psychologist; **ART,** Argumentos de Razón Técnica; **ASR**, American Sociological Review; **CB**, Cyberpsychology & Behavior; **CDJ**, Cuadernos de Derecho judicial; **CICJ,** Current Issues in Criminal Justice; **DB**, Deviant Behavior; **EJC**, European Journal of Criminology; **EREL**, Espéculo. Revista de estudios literarios; **FMPRJI**, First Monday Peer-Reviewed Journal on the Internet; **ICS**, Information Communications and Society; **IJCC**, International Journal of Cyber Criminology; **IECS**, International E-journal of Criminal Science; **IJCSIS**, International Journal of Computer Science and Information Security; **IS**, The Information Society; **JCLC**, The Journal of Criminal Law and Criminology; **JRCD**, Journal of Research in Crime and Delinquency; **JSS**, Journal of Strategic Security; **LL**, La Ley Penal. Revista de Derecho penal, procesal y penitenciario; **LNCS**, Lecture Notes in Computer Science; **OSJCL**, Ohio State Journal of Criminal Law; **PHG**, Progress in Human Geography; **PSPB**, Personality and Social Psychology Bulletin; **RCVS**, Rivista di Criminologia, Vittimologia e Sicurezza; **RDPC,** Revista de Derecho penal y Criminología; **RFDUCM**, Revista de la Facultad de Derecho de la Universidad Complutense de Madrid; **SJ**, Security Journal; **SLS**, Social & Legal Studies; **SM,** Science Magazine; **SSCR**, Social Science Computer Review; **TJMJCIL**, The John Marshall Journal of Computer & Information Law, **TSoc.**, Time and Society; **VJOLT**, Virginia Journal of Law & Technology.

[1] Véase, por ejemplo, DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.):*Derecho penal informático,* Civitas, Cizur Menor, 2010. En nuestro país institucionalmente se prefiere esa denominación para, por ejemplo, la fiscalía delegada en materia de delitos informáticos.

[2] Entre los primeros, THOMAS, D./LOADER, B.: "Introduction – Cybercrime: Law enforcement, security and surveillance in the information age", en THOMAS, D./LOADER, B. (EDS.): *Cybercrime: Law enforcement, security and surveillance in the information age*, Routledge, London, 2000; y FURNELL, S.: "Cybercrime: vandalizing the information society", en *LNCS,* vol. 2722, 2003, p.333, donde señala que el crimen informático no anticipaba el riesgo que conllevaría la generalización del uso de estas tecnologías que ha supuesto Internet.

[3] Conviene recordar que el prefijo *cyber* proviene a su vez del término *cyberspace* creado por el novelista de ciencia ficción William GIBSON y su obra *Neuromancer,* AceBooks, New York, 1984, (en España, traducida "Neuromante"), en la que el autor describía una sociedad tecnológicamente avanzada en la que las personas vivían en un mundo virtual separado del mundo real.

espacio de significado, tales como *computercrime* y otros en los que se utilizan prefijos como *virtual*, *online*, *high-tech, digital, computer-related, Internet-related, electronic*, y *e-crimes*[4]. En la raíz de este cambio de denominación está, a mi parecer, la mayor capacidad del término cibercrimen para expresar la característica esencial que une a esta forma de criminalidad y que la diferencia de otro tipo de delincuencia[5]. Me refiero a que la primera se realiza en un nuevo ámbito o espacio con características estructurales intrínsecas y extrínsecas tan distintas a las del espacio físico en el que se ejecuta la delincuencia tradicional, que obliga a una revisión criminológica de la explicación del evento delictivo, así como una adaptación de las normas jurídicas para su mejor prevención. La denominación delitos informáticos o *computercrimes* expresaba perfectamente la preocupación por un nuevo tipo de delincuencia surgida con la aparición de los primeros sistemas informáticos, en la que éstos eran el medio o el objetivo del crimen. Como ha señalado Wall[6], la generación de delitos que nos interesan ya no preocupan por tener como elemento característico el realizarse desde ordenadores, sino por el hecho de que tales sistemas informáticos estén conectados en un ámbito de comunicación transnacional-universal, el ciberespacio, y porque sea en ese nuevo "lugar" en el que, desde cualquier espacio físico ubicado en cualquier Nación, se cometen infracciones que pueden afectar, en lugares distintos y simultáneamente, a bienes jurídicos tan diversos como el patrimonio, la intimidad, la libertad y la indemnidad sexuales, el honor, la dignidad personal, la seguridad del estado, la libre competencia, entre otros muchos[7].

El objeto de este trabajo es el cibercrimen, porque el objetivo es analizar en qué medida el ciberespacio se configura como un nuevo ámbito de oportunidad criminal que obliga a repensar las estrategias de prevención de la delincuencia en él cometida y de qué forma podemos adaptar las enseñanzas de la Teoría de las Actividades Cotidianas[8] (en adelante, TAC) a ese distinto "lugar" de comisión delictiva. Con esta intención adopto, pues, un concepto amplio de cibercrimen, como cualquier delito en el que las TIC juegan un papel determinante en su concreta comi-

[4] SMITH, R. G./GRABOSKY, P./URBAS, G.: *Cyber criminals on trial,* Cambridge University Press, Cambridge, 2004, p. 5.

[5] Que es lo que, como señala YAR, debe ser el propósito esencial de cualquier concepto que sirve para nombrar a una categoría: enfatizar aquello que une a todo aquello que la conforma, en este caso, Internet y las TIC como medio de comisión delictiva. YAR, M.: "The novelty of 'cybercrime': an assessment in light of routine activity theory", en *EJC,* núm. 2, 2005, p. 409.

[6] WALL, D.: *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge, 2007, pp. 44 y ss.

[7] CLOUGH, J.: *Principles of Cybercrime,* Cambridge University Press, Cambridge, 2010, p. 4.

[8] Su primera formulación en COHEN, L./FELSON, M.: "Social change and crime rate trends: A routine activity approach", en *ASR,* vol. 44, núm. 4, 1979, pp. 588–608. Esta teoría ha sido traducida tradicionalmente como teoría de las actividades rutinarias (Véase, por todos, SERRANO MAÍLLO, *Introducción a la criminología*, 6ª ed., Dykinson, Madrid, 2009, pp. 310 y ss.). Sin embargo, he preferido referirme a ella en castellano como teoría de las actividades cotidianas porque, como ha señalado el propio FELSON en nuestro país, el concepto de "lo cotidiano" refleja mucho mejor que el de "rutina" lo que pretende expresar la teoría, de que es en el actuar del día a día, en el comportamiento cotidiano de cada sujeto, donde se produce cualquier delito. La palabra rutina tiene una connotación peyorativa que no tiene la palabra cotidiano y que no es necesaria para la descripción del significado de la teoría.

sión, que es lo mismo que afirmar que será tal cualquier delito (comportamiento humano que conforme a las normas jurídicas debiera ser enjuiciado como delictivo) llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan[9].

Al hablar de cibercrimen o cibercriminalidad, por tanto, lo hago para referirme a una macrocategoría, parelela (aunque situada dentro de ella a la vez) a la de crimen o criminalidad, y únicamente diferenciada de ésta por no ejecutarse en el espacio físico, sino en el ciberespacio. En ella caben, desde una perspectiva fenomenológica, tanto los delitos que únicamente podrían ser realizados por la existencia del ciberespacio (o cibercrímenes puros, tales como el *hacking,* ataques DoS, infecciones de Malware, y demás que no existirían como infracciones de no hacerlo las TIC), como los delitos que también tienen una modalidad de comisión en el espacio físico si bien en la concreta modalidad de ejecución en el ciberespacio (ciberfraudes de distinta naturaleza, ciberacoso sexual a menores, *cyberbullying*, *cyberstalking*, entre otros muchos), incluyendo dentro de éstos una particular, que podría ser tercera, categoría de infracciones, cuya ilicitud se caracteriza por la prohibición de la transmisión o difusión del contenido (pornografía infantil, *hatespeech* o difusión de mensajes de odio racial, ciberterrorismo, piratería intelectual en Internet, etc.); y todos ellos, bien sea la finalidad del cibercriminal la económica, política o ideológica ,social o personal, en el marco de la utilización de las TIC en la web 2.0 como instrumentos para las relaciones personales y la creación de redes y grupos sociales. Qué duda cabe, que cada una de estas grandes categorías, incluso cada uno de los crímenes, conllevará unas problemáticas criminológicas distintas. Tampoco debe olvidarse, y esto es ahora lo esencial, que a todos esos delitos les une algo que, además, les va a caracterizar frente a los crímenes en el espacio físico, el lugar, nuevo, en el sentido de distinto, en el que se cometen.

2. **EL CIBERESPACIO COMO NUEVO ÁMBITO DE OPORTUNIDAD CRIMINAL**

Las TIC, en general, e Internet como red global, en particular, han supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica, que ha sido denominado El Ciberespacio[10], y respecto al cual nos debemos plantear si el mismo puede definirse como un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional

[9] De modo similar JEWKES, define el cibercrimen como cualquier acto ilegal cometido por medio de (o con la asistencia de) sistemas informáticos, redes digitales, Internet y demás TIC. JEWKES, Y.: "Cybercrime", en MCLAUGHLIN, E.U./MUNCIE, J. (EDS.).:*The Sage Dictionary of Criminology,* Sage, London -California, 2006, p. 106.

[10] Aunque no son lo mismo Internet, la WWW y el ciberespacio, (véase De ANDRÉS BLASCO, J.: "¿Qué es Internet", en GARCÍA MEXÍA, P. (DIR.):*Principios de Derecho de Internet,* Tirant lo Blanch, Valencia, 2002, p. 29) en este artículo se utilizan en muchos casos los términos ciberespacio, Internet y La Red, como equivalentes, cuando no es necesaria ninguna precisión de diferenciación entre estos conceptos.

físico tradicional o, por el contrario, idéntico a éste en sus caracteres esenciales. Siguiendo la acertada metáfora de Grabosky, la cuestión es ¿en qué sentido el cibercrimen es "old wine in new bottles"?[11]: puede serlo en el de constituir un tipo de delincuencia esencialmente nueva y respecto de la cual no son válidas las teorías criminológicas aplicables al delito llevado a cabo en el espacio físico-nacional; o en el de tratarse de la misma delincuencia con un aspecto diferente pero para la que son válidas las mismas teorías y los mismos instrumentos usados frente al crimen en el espacio físico; y también, por último, puede tratarse de una criminalidad con elementos configuradores idénticos pero que se ven afectados, de forma esencial, al plasmarse en el ciberespacio, de modo tal que ello puede influir significativamente en la explicación del delito y, por tanto, en su prevención.

Sin entrar todavía en el fondo de estas cuestiones sí puede adelantarse lo obvio: que el crimen, como cualquier otro evento social, cambia en Internet, por lo menos si integramos en la comprensión del evento el lugar en el que el mismo se produce. Si, como señalaran hace ya más de tres décadas Cohen y Felson[12], el crimen se produce cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y sin un guardián capaz de darle protección al primero, es evidente entonces que los especiales caracteres del ciberespacio en los que se ven modificados los parámetros espacio-temporales, pueden incidir en una modificación de los condicionantes del delito. Voy a tratar, por tanto, de analizar en qué cambia el ciberespacio, cuáles son las singularidades de ese nuevo espacio que conllevan que cualquier evento social en él se caracterice de forma distinta a como lo es en el otro espacio de comunicación social, antes de tratar de adivinar cómo influye ello en el evento social que es el (ciber)crimen.

2.1. **Caracteres del ciberespacio**

2.1.1. ***Caracteres intrínsecos: Tiempo y espacio en el ciberespacio***

Tiempo y espacio son coordenadas de cualquier fenómeno social, de modo que en la configuración de éste son elementos definitorios o inherentes al mismo. Por ello si tales elementos se ven modificados en relación con un determinado fenómeno en comparación con otro, podemos afirmar que su concreta expresión se convierte en caracteres intrínsecos del mismo. Es lo que ocurre con el ciberespacio como ámbito social que tiene como caracteres intrínsecos una concreta configuración de las coordenadas espacio/tiempo, frente a la que tienen en el que podríamos denominar espacio real o físico.

Ha advertido con acierto Graham, que se suele acudir a la geografía para utilizar

[11] GRABOSKY, P.: "Virtual Criminality: Old Wine in New Bottles?", en *SLS,* núm. 10, 2001, pp. 243 y ss., también BRENNER, S. W.: "Cybercrime Metrics.Old Wine, New Bottles?", en *VJOLT***,** vol. 9, núm. 13, 2004,pp. 1 y ss.

[12] COHEN, L./FELSON, M.: "Social change…", *ob. cit.,* pp. 588–608.

metáforas sobre los nuevos ámbitos de comunicación surgidos en la sociedad de la información. Ocurre con el propio término ciberespacio, pero también con otros como el sitio web, la comunidad virtual, o la autopista de la información[13]. En realidad estas metáforas, geográficas o sociales, ayudan a visualizar, en términos de funcionalidad social, lo que, en última instancia, no son más que circuitos de señales electrónicas que contienen información codificada. Tales palabras se convierten así, en herramientas conceptuales utilizadas para entender el sentido y alcance funcional de una nueva tecnología; para traducir estas nuevas técnicas en términos de cuál es el uso social que se puede hacer de ellas, cuáles son los efectos de su desarrollo, y cuáles sus diferencias con las tecnologías anteriores. En el caso del término ciberespacio, el mismo sirve para poner de manifiesto que se trata de un lugar de comunicación que no tiene una naturaleza física primaria, sino esencialmente relacional. 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[14].

Se suele utilizar como sinónimo de ciberespacio el concepto de "espacio 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[15]. 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. 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[16]. El espacio se contrae, la intercomunicación se expande[17]. Y mientras que hasta el momento era necesario que las dos ocupasen (prácticamente) el mismo espacio para poder comunicarse, ahora pueden hacerlo al mismo tiempo (o en tiempos separados, sobre lo que trataré después) y en el mismo (ciber)espacio, pero en distintos espacios geográficos (o a distancia).

[13] GRAHAM, S.: "The end of geography or the explosion of place? Conceptualizing space, place and information technology", en *PHG,* vol. 22, núm.2, 1998, pp. 165 y ss.

[14] AGUIRRE ROMERO, J. Mª: "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI", en *EREL*, Universidad Complutense de Madrid, núm. 27, julio/octubre, 2004, en Internet en http://www.ucm.es/info/especulo/numero27/cibercom.html. Citado el 1 de octubre de 2010.

[15] GUTIÉRREZ PUEBLA, J.: "Redes, espacio y tiempo", en *AGUC,* núm. 18, 1998, p. 81.

[16] GUTIÉRREZ PUEBLA, J.: "Redes, espacio…", *ob. cit.,* p. 65.

[17] Así, GREEN, N.: "On the Move: technology, mobility, and the mediation of social time and space", en *IS*, vol. 18, núm. 4, 2002, p. 285, quien señala que hay una compresión espacio-temporal, en el sentido de la reducción del tiempo necesario para cubrir una distancia, pero un estiramiento en el sentido de que aumenta el contacto entre las sociedades.

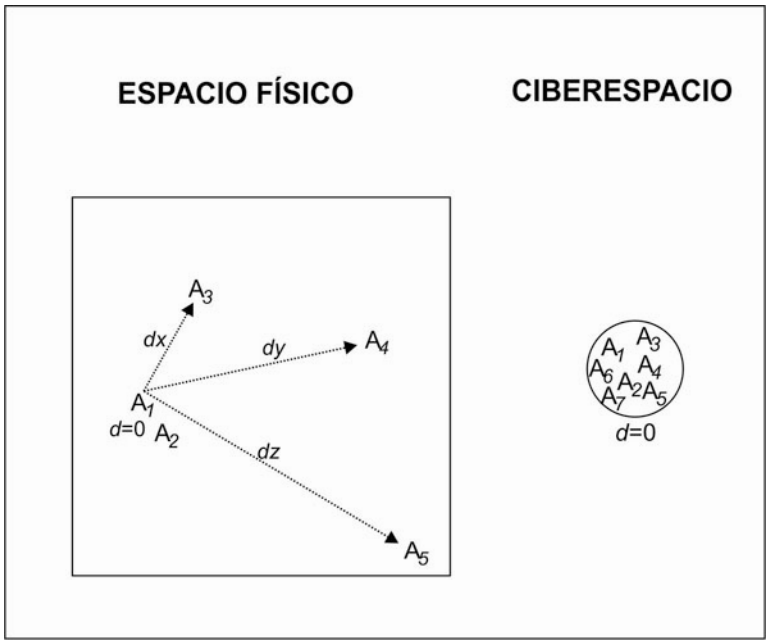


Gráfico 1. **Contracción de la distancia en el ciberespacio y expansión de la capacidad comunicativa:** A1 necesita d=0 para comunicarse con A2, A3, A4, etc.

Si Internet ha supuesto la creación de un nuevo espacio, también puede afirmarse que en él cambia el tiempo, su percepción social, así como la forma en la que el mismo tiempo se organiza[18]. De hecho, la incidencia de las TIC en el espacio se plasma irremediablemente en el tiempo. 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[19]. 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"[20], dado que en Internet los eventos suceden mucho más rápidamente que en la vida no virtual[21]. 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, como señaló Giddens, el avance de las TIC ha permitido salvar las "distancias temporales" entre las sociedades y acercarlas hasta convertir el contacto entre ellas

[18] LEE, H./LIEBENAU, J.: "Time and the Internet at the turn of the millenium", en *TSoc.,* vol. 9, núm. 1, 2000, p. 44.

[19] KITCHIN, R. M.: "Towards geographies of cyberspace", en *PHG,* vol. 22, núm. 3, 1998, p. 386.

[20] GREEN, N.: "On the Move...",*ob. cit.,* p. 284.

[21] Me parece muy gráfico el ejemplo de WELLMAN, B.: "Computer Networks As Social Networks", en *Science*, vol. 293, 14 de septiembre de 2001, p. 2034, cuando señala que "an Internet year is like a dog year, changing approximately seven times faster than normal human time".

en algo instantáneo[22]. Como se ve en el Gráfico 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.

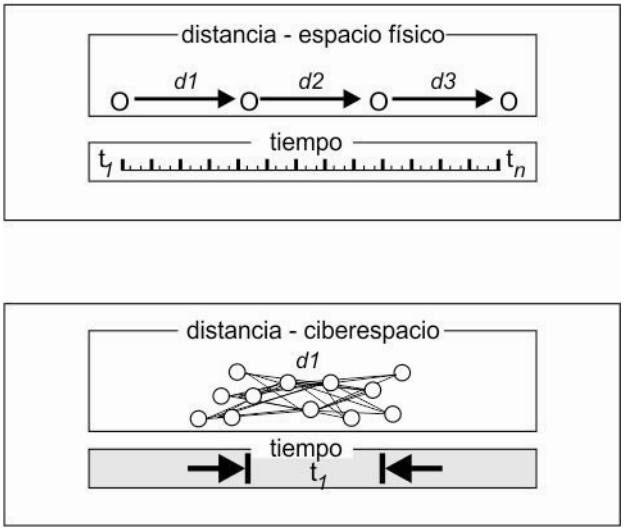


Gráfico 2. **Contracción del tiempo.** El tiempo necesario para la comunicación disminuye al no existir distancias en el ciberespacio.

Por otra parte, el factor tiempo, cuando se da en el espacio virtual, se puede ver modificado en un sentido distinto a lo acabado de reflejar. Concretamente, el ciberespacio puede convertir en perenne lo que en el espacio físico es instantáneo y caduco. Esto ocurre con los efectos de los actos en el ciberespacio: los comportamientos realizados a través de él, especialmente aquellos consistentes en la publicitación de contenidos, pueden quedar fijados durante un tiempo indeterminado y seguir desplegando efectos aunque su ejecución sólo haya durado un instante. Además, y como adelantábamos al tratar la mutación del elemento espacio en Internet, 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 el Gráfico 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 indeterminado 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.

[22] FUCHS, C.: "Transnational Space and the "Network Society", en *Paper Presented at the Association of Internet Researchers (AoIR) Conference: Internet Research 7.0,* Brisbane, September 27-30, 2006, en Internet en http://aoir.org/files/fuchs_516.pdf, p. 9. Citado el 2 de diciembre de 2010.

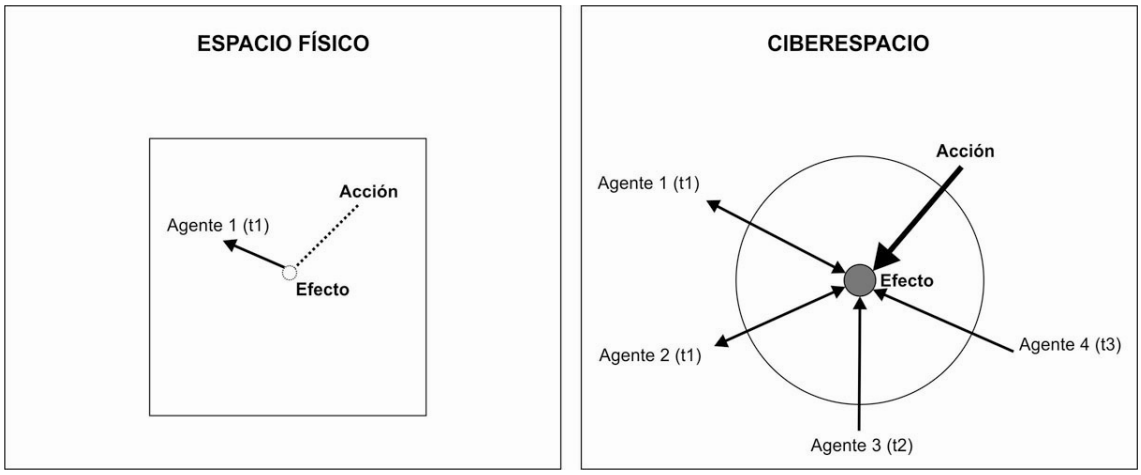


Gráfico 3. **Fijación de los efectos en el ciberespacio.** La acción se ejecuta en un momento x, pero A3 y A4 interaccionan con ella en momentos posteriores.

Lo que se ve afectada por estos cambios, por tanto, es la capacidad de control por parte del agente del hecho en relación con el elemento temporal, así como la de los agentes que interaccionan con lo realizado. Y lo mismo sucede con el elemento espacial: en el espacio físico el agente activo 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 es casi imposible saber quién, desde cualquier lado del mundo, se verá afectado por los mismos. Por ello, 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. 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.

En definitiva, y a los efectos que más nos interesan, 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. 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 de las coordenadas espacio/temporales del acto al que se deben atribuir las mismas y, por ello, del agente causante, que en el espacio físico.

2.1.2. *Algunos caracteres extrínsecos (pero configuradores) del ciberespacio*

El ciberespacio, por serlo, está configurado en sus coordenadas espacio/temporales de forma distinta al espacio físico. Además de ello, este nuevo ámbito social configurado por Internet y las TIC, tiene otros muchos caracteres que hoy en día se consideran absolutamente definitorios, si bien podrían ser distintos a los que son[23]. El que se trate de caracteres extrínsecos no obsta, sin embargo, para que podamos afirmar de algunas de las características que vamos a analizar a continuación, que las mismas son esenciales o configuradoras de lo que en la "conciencia colectiva" se definiría como el ciberespacio. Sin la transnacionalidad del ciberespacio, esto es, con un ciberespacio en el que existieran fronteras y hubiera que pasar de uno a otro; sin su descentralización, sin su carácter universal y abierto, o sin el efecto de mutación constante que sobre sus funcionalidades causa el desarrollo tecnológico, el ciberespacio no sería el que es como ámbito de intercomunicación social y no modificaría, como lo hace, los caracteres del evento social que es el crimen.

a) Deslocalización, transnacionalidad, neutralidad y descentralización

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 he analizado anteriormente. No puede negarse, sin embargo, que tal carácter no tendría la importancia que tiene si no viniera unido

[23] Véanse los citados por CAPELLER, W.: "Not such a neat net: some comments on virtual criminality", en *SLS,* núm. 10, 2001, p. 233.

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. Me refiero, obviamente a la transnacionalidad del ciberespacio, a la inexistencia de fronteras o distancias[24], aparentes, o reales, en un *microcosmos* 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. Aumentan por tanto, en el ciberespacio, las facilidades para la multicomunicación social (transnacional), y disminuyen, así, los impedimentos para la comunicación entre personas (así como entre bienes), cuanto menos el que la misma se limitaba a las personas que se hallasen físicamente próximas.

Otro carácter extrínseco de la 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[25]. 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 que Estados u organizaciones pretendan definir un ciberespacio distinto.

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

[24] PÉREZ LUÑO, A. E.: "Impactos sociales y jurídicos de Internet", en *ART,* núm. 1, 1998.

[25] ALCANTARA, J.: *La neutralidad en La Red, y porqué es una mala idea acabar con ella*, Biblioteca de Las Indias, 2011.

distribuido, dado que en la estructuración de Internet no existen nodos centrales, pero tampoco nodos que actúen como centros locales, sino que se trata, como ha señalado gráficamente Alcántara, de una malla "en la que ningún nodo tiene el poder de aislar a otro, en la que ningún nodo tiene el poder de decidir qué conecta con qué", y en la que, por tanto, la caída de un nodo no imposibilita que la información siga fluyendo[26]. 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[27]. 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.

b) El ciberespacio 2.0: universal, popularizado y anonimizado

También debe destacarse del ciberespacio su carácter universal, y no en este caso en el sentido de transnacional, sino en el de global, colectivo o popular. Al fin y al cabo, son las gigantescas dimensiones de ese nuevo espacio de comunicación social, las que le otorgan una dimensión de riesgo que, en el caso de tener un ámbito más reducido, no tendría. En el mundo podemos hablar de aproximadamente mil millones de usuarios, y si bien hubo un momento en que los sistemas informáticos eran únicamente utilizados por empresas o instituciones públicas con fines de negocios, la popularización de la informática y el aumento de las facilidades para adquirir o acceder a terminales, ha generalizado el uso del ciberespacio por particulares[28], y la unión de todo ello con los nuevos servicios para la comunicación social, especialmente las redes sociales, ha inaugurado un nuevo ciberespacio, la Web 2.0, en la que Internet es ya el más importante vehículo de comunicación personal y un instrumento esencial para la vida social.

La universalización de Internet, su popularización como espacio de intercomunicación personal, también tiene que ver, además de con su bajo coste, con el anonimato que el mismo confiere[29]. Aunque se digapor parte de algún autor, que el anonimato no es ya una característica de Internet al ser cada vez más sencilla la

[26] ALCANTARA, J.: La neutralidad..,*ob. cit*.

[27] ROMEO CASABONA, C. M.: "De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal", en ROMEO CASABONA, C.M. (COORD.):*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Comares, Granada, 2006, p. 3.

[28] CLOUGH, J.: *Principles of Cybercrime, ob. cit.,* p. 6.

[29] LÓPEZ ORTEGA, J. J.: "Libertad de expresión y responsabilidad por los contenidos en Internet", en *CDJ,* núm. 10, 2001, p. 119.

identificación de las direcciones IP[30], lo cierto es que sigue siendo en la actualidad más compleja, pese a los rastros digitales del delito, la identificación de los autores de estas conductas que la de otros sujetos que cometen similares infracciones pero en el mundo real[31]. Si a la todavía compleja determinación del sujeto con la concreción de la IP, unimos la existencia de los cibercafés desde los que comunicarse en el ciberespacio, redes *wifi* que permiten acceder desde sitios abiertos, proveedores de servicios gratuitos que no exigen la identificación de los usuarios[32], múltiples sistemas que permiten enviar correos electrónicos de forma anónima[33] 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, etc., concluiremos que el ciberespacio puede seguir siendo un ámbito para la intercomunicación anónima.

c) El ciberespacio abierto y sujeto a revolución permanente

Tampoco hay que desdeñar la importancia de que las TIC se caractericen 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. 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, 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. En el espacio físico esto puede suceder, pero es obvio que en el ciberespacio en el que la evolución tecnológica se muestra como revolución imparable, la necesaria actualización de los sistemas de protección se hace imprescindible pero compleja.

Además, Internet está configurando 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[34]. Incluso aquellos que no tienen

[30] WALL, D.: "Cybercrime and the culture of fear: Social Science fiction(s) and the production of knowledge about cybercrime", en *ICS*, vol. 11, núm. 6, 2008, pp. 874 y ss.

[31] ZHENG, R./QIN, Y./HUANG, Z./CHEN, H.: "Authorship Analysis in Cybercrime Investigation", en VV.AA.: *Lecture notes in computer science,* Springer Verlag, Berlin-Heidelberg, 2003, p. 59. También, DE LA MATA BARRANCO, N. J.: "Ilícitos vinculados al ámbito informático: la respuesta penal", en DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.): *Derecho penal informático, ob. cit.,* p. 19, nota 10.

[32] LÓPEZ ORTEGA, J. J., "Libertad de expresión…, *ob. cit.,* p. 119.

[33] Véanse los detallados por PITTARO, M. L.: "Cyber stalking: An Analysis of Online Harassment and Intimidation", en *IJCC*, vol. 1 ,núm. 2, 2007, p. 1815.

[34] CAPELLER, W.: "Not such a neat net...",*ob. cit,* p. 233.

experiencia en la utilización de los sistemas informáticos, y por supuesto quienes poseen estos conocimientos y tienen inquietudes relacionadas con el mundo virtual, pueden, mediante sus creaciones (véanse los casos de Youtube o Facebook), o sus usos (los mismos), cambiar la forma de comunicación social en el ciberespacio, de modo tal que el usuario se siente parte definitoria del ciberespacio y, por tanto, parte decisoria del mismo, especialmente en su configuración como espacio de libertad. 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 sólo 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 sea cierto aquello generalmente aceptado relativo a que a mayor correspondencia entre lo normado y lo aceptado socialmente, mayor cumplimiento de las normas[35].

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 criminal en el ciberespacio**

2.2.1. ***Criminología del cibercrimen y revisión de la oportunidad y las actividades cotidianas en el ciberespacio***

Las primeras aproximaciones de la criminología al fenómeno del cibercrimen se centraron en la discusión acerca de las motivaciones del *hacker*, quizás por lo atractivo que resultaba ese personaje que cometía delitos y que, sin embargo, parecía tan alejado del prototipo de delincuente, pero también por focalizarse en aquellos momentos la criminología en el sujeto criminal, en la comprensión de los condicionantes de su conducta y sus modalidades. En los últimos años, sin embar-

[35] Véanse en este sentido los trabajos de CIALDINI y colaboradores (CIALDINI, R.B./KALLGEREN, C.A./RENO, R.R: "A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior", en *Advances in Experimental Social Psychology,* núm. 24, 1991, pp. 201-234; y CIALDINI, R.B./KALLGEREN, C.A./RENO, R.R. (2000): "A focus theory of normative conduct: When norms affect and do not affect behavior", en *Personality and Social Psychology Bulletin*, vol. 26, núm. 8, pp. 1002-1012,queponen de manifiesto las condiciones en las que los tipos de influencia social informativa y normativa son más eficaces sobre el comportamiento que la norma. Otro factor que aparece relacionado con el cumplimiento de la ley, es la legitimidad percibida de la norma y de las autoridades, tal y como se refleja en los trabajos de TYLER (TYLER, T.R.: *Why people obey the law*, Princeton University Press, Princeton, 2006) y que actuaría motivando el cumplimiento de manera voluntaria, independientemente de las sanciones o penas asociadas a la transgresión. Véase también, TYLER, T.R.: "Legitimacy and criminal justice: The benefits of self-regulation", en *Ohio State Journal of Criminal Law,* núm. 7, 2009, pp. 307-359.

go, el enfoque ha cambiado, y si bien podemos encontrar interesantes estudios de criminología aplicada a la cibercriminalidad en las que se manejan teorías de la criminalidad como la del autocontrol[36], la decisión racional[37], la del aprendizaje social[38], el control social[39] o el etiquetamiento[40], gran parte de los estudios criminológicos que tratan de comprender el crimen en Internet y de, incluso, definir los caracteres particulares de este evento por el hecho de llevarse a cabo en el ciberespacio, toman en consideración para su análisis el "approach" de la oportunidad y, más concretamente, la TAC de Cohen y Felson[41].

A primera vista puede resultar curioso que sea esta teoría, influyente, pero como otras, la que se haya convertido en el principal constructo desde el que analizar las especialidades del crimen en el ciberespacio[42]. En realidad, hay varios factores que, a mi parecer, explican esto y que van más allá de su propio atractivo intrínseco derivado de la unión de sencillez y gran fuerza expresiva[43].

En primer lugar, ya hace tiempo que se puede constatar que la criminología ha

[36] HIGGINS, G. E./FELL, B. D./WILSON, A. L.: "Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States", en *SSCR,* núm. 25, 2007, pp. 339 y ss. Aunque sea para un fenómeno delictivo muy concreto, este trabajo es especialmente interesante porque también utiliza y compara, para el caso de la piratería intelectual, la teoría del aprendizaje social. Véase también al respecto, y en sentido prácticamente idéntico, HIGGINS G. E./MAKIN D. A.: "Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy?", en *IJCC,* primavera, vol. 2, 2004.

[37] En realidad, y por motivos obvios derivados de la relación entre la teoría de la elección racional y las teorías de la oportunidad, la mayoría de los trabajos en los que se analiza la incidencia del cibercrimen en el modelo teórico de la decisión racional, llevan a cabo su análisis junto con el de otras teorías como la de las actividades cotidianas o referidas a la prevención situacional. Así ocurre, por ejemplo, con BEEBE, N. L./RAO, S. V: "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security", en *Proceedings of the 2005 SoftWars Conference,* Las Vegas, NV, Dec 2005.

[38] YOUNG, R./ZHANG, L.: "Factors Affecting Illegal Hacking Behavior", en **AMCIS 2005 Proceedings, p**aper 457, 2005, en Internet en http://aisel.aisnet.org/amcis2005/457. Citado el 3 de diciembre de 2010; donde también se tiene en cuenta el enfoque del control social.

[39] SVENSSON, J. S./BANNISTER, F.: "Pirates, sharks and moral crusaders: Social control in peer–to–peer networks", en *FMPRJI,* vol. 9, núm. 6 – 7, junio, 2004, pp. 1 y ss.

[40] En el *labeling approach* se basa el estudio de TURGEMAN-GOLDSCHMIT, O.: "Meanings that Hackers Assign to their Being a Hacker", en *IJCC*, vol. 2, julio-diciembre, 2008, pp. 382 y ss.

[41] COHEN, L./FELSON, M.: "Social change...", *ob. cit.,* pp. 588–608. El enunciado esencial de la teoría sería que el crimen se produce durante los actos cotidianos del día a día, cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y sin un guardián capaz de darle protección al primero.

[42] Véase así, YAR, M.: "The novelty of 'cybercrime'....",*ob.cit,* pp. 407-427; CHOI, K.: "Computer Crime, Victimization and Integrated Theory: An Empirical Assessment", en *IJCC,* vol. 2, enero-junio, 2008, pp. 308 y ss.; HUTCHINGS, A./HAYES, H.: "Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?", en *CICJ*, vol. 20, núm. 3, marzo, 2009, pp. 433 y ss.; HOLT, T. J./BOSSLER, A. M..:"Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization", en *DB*, vol. 30, núm. 1, enero, 2009, pp. 1 y ss.; HOLT, T. J/BOSSLER, A. M.: "On-line Activities, Guardianship and Malware Infection: An Examination of Routine Activities Theory", en *IJCC,* vol. 3, núm. 1, enero-junio, 2009, pp. 400 y ss.; YUCEDAL, B.: "Victimization in cyberspace: An application of routine activity and lifestyle exposure Theories", 2010, en Internet en http://etd.ohiolink.edu/send-pdf.cgi/YUCEDAL%20BEHZAT.pdf?kent1279290984. Citado el 9 de septiembre de 2010, pp. 26 y ss. Como se puede observar ya sólo en los títulos de los artículos, gran parte de ellos centran el estudio en las implicaciones victimológicas de esta teoría. No es de extrañar si tenemos en cuenta que hay quienes la conciben esencialmente así, y si tenemos en cuenta que su aporte de la oportunidad sitúa al *suitable target* en el centro de la problemática criminológica. Esto hará que posteriormente, cuando analicemos las consideraciones victimológicas de la cibercriminalidad, volvamos sobre algunas de estas referencias y sobre la RAT.

[43] Así, también, TILLEY, quien dice que un primer vistazo a la teoría, puede hacer que la misma parezca banal, pero que ésta sirvió para poner de manifiesto que era posible aplicar políticas y prácticas reales tendentes a modificar tales factores y, por tanto, a prevenir el delito. TILLEY, N.: *Crimeprevention*,Willan Publishing, Collumpton, 2009, p. 122.

centrado su foco en el crimen como evento, completo y complejo[44], que conlleva la constatación de un espacio de oportunidad criminal cuya identificación y análisis puede ser esencial a efectos preventivos. La TAC es, sin lugar a dudas, parte del germen de este cambio de visión de la criminología y, en particular,de las teorías de la oportunidad o del día a día[45] 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[46] y que han dado lugar, en conjunción con la teoría de la decisión racional[47], a los desarrollos sobre la prevención situacional del delito.

[44] La idea del crimen como evento está tomando fuerza en los últimos años como forma de unión de los aportes de las nuevas teorías de la oportunidad con los desarrollos de la criminología tradicional; MEIER, R. F./KENNEDY, L. W./SACCO, V. F.: "Crime and the criminal event perspective", enMEIER, R. F./ KENNEDY, L. W./SACCO, V. F. (EDS.): *The Process and structure of Crime. Criminal events and Crime analysis, Advances in Criminological Theory*, vol. 9, Transaction Publishers, New Jersey, 2001, pp. 3 y ss. En ésta, como han señalado BRANTHINGHAM y BRANTHINGHAM, el foco se seguía situando en las motivaciones y las conductas de los criminales, hasta el punto de excluir en la mayoría de los casos cualesquiera otras consideraciones, siendo, por tanto, el avance, el permitir abrir la criminología al estudio de todos sus componentes, entre otros el rol criminógeno desempeñado por las propias víctimas y objetivos, por guardianes y gestores, etc. BRANTHINGHAM, P. J. /BRANTHINGHAM, P.: "The implications of the criminal event model for crime prevention", en MEIER, R. F./KENNEDY, L. W./SACCO, V. F. (EDS.): *The Process and structure…, ob. cit.,* pp. 277 y ss. Aunque la idea del crimen como evento se atribuye a autores como MEIER, SACCO, KENNEDY, GIBBS VAN BRUNSCHOT o EKBLOM, es evidente que la misma debe mucho a la TAC de COHEN y FELSON, como reconocen entre otros, KENNEDY, L.W./GIBBS VAN BRUSCHOT, E.: "Routines and the criminal event", en MEIER, R. F./KENNEDY, L. W./SACCO, V. F. (EDS.): *The Process and structure…, ob. cit.;* así como BRANTHINGHAM, P. J./BRANTHINGHAM, P.: "The implications of the criminal…", *ob. cit*., p. 278.Recientemente, en nuestro país, se ha editado un extraordinario trabajo de revisión de la oportunidad y su significado criminológico, en el que se adopta la perspectiva del crimen como evento, si bien desde la base del filósofo analítico Donald DAVIDSON, (DAVIDSON, D.: *Essays on actions and events,* ClarendonPress, Oxford, 1980) por medio de una "metateoría" que entiende que no es posible integrar (ni interaccionar entre sí) la motivación y la oportunidad en una teoría, dado que ambos elementos no son más que descripciones de un mismo evento, el evento criminal o, en otras palabras, una misma cosa bajo distintas descripciones. SERRANO MAÍLLO, A.:*Oportunidad y delito,* Dykinson, Madrid, 2009, pp. 200 y ss., especialmente 205, también 210 y ss., y 220 y ss., concretamente 224. No podemos pronunciarnos aquí, aunque trataremos de hacerlo más adelante, al respecto de esta aportación. Resulta especialmente interesante, en todo caso, y a los efectos que nos interesa, su consideración, como otros, de la TAC como una teoría de la victimización, y la influencia en ella de la Teoría de los estilos de vida, de HINDELANG, M. J./GOTTFREDSON, M. R./GAROFALO, J.: *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*, Cambrdige, MA, Balliger Publishing Company, 1978, pp. 240 y ss.

[45] Se suelen considerar como grandes hitos de las teorías de la oportunidad, dos trabajos publicados a finales de los años 70 en Londres y EEUU: por una parte, el trabajo monográfico de MAYHEW, P./CLARKE, R./STURMAN, A./HOUGH, M.:*Crime as opportunity, Home office Research Study,* núm.34, London, 1976, y por otra, el ya citado trabajo de COHEN y FELSON, "Social change …", *ob. cit.* Al respecto, señala TILLEY, N.: *Crime Prevention, ob. cit.,* p. 120, que las dos teorías surgieron al mismo tiempo, debiendo considerarse el desarrollo de la TAC, independiente del británico, al no existir en aquellos momentos referencias del trabajo realizado al otro lado del Atlántico. Lo cierto es que si bien el planteamiento era diverso, ambas convergían en las bases de las que partían (la decisión racional) y en la voluntad de situar el acento de la prevención y de la explicación del delito, no sólo en el criminal, sino también en el espacio y el tiempo en el que él actúa, como demuestran trabajos posteriores en los que se unen CLARKE y FELSON, como en CLARKE, R. V./FELSON, M.: "Introduction: Criminology, routine activity, and rational choice", en CLARKE, R./FELSON, M.(EDS.): "Routine activity and rational choice", en *ACT,* vol. 5, TransactionPublishers, New Brunswick, New Jersey, 1993. Tampoco habría que desdeñar la importancia en el paradigma de la oportunidad de uno de sus primeros antecedentes, incluso anterior a la teoría de las actividades cotidianas de COHEN y FELSON, si bien restringida al papel de la víctima y centrada en la explicación de su victimización a partir de factores demográficos, como es la Teoría de los estilos de vida de HINDELANG, que vino a ser la primera que incorporó al análisis del crimen, el tópico de la víctima. La misma, ya argumentaba que las elecciones individuales de la víctima, tales como con quién se reunía y por dónde, qué tipo de ocio frecuentaba, etc., influían en el riesgo de victimización. (HINDELANG, M. J./GOTTFREDSON, M. R./GAROFALO, J. : *Victims of personal…, ob. cit.,* p. 242).

[46] Véase sobre la "environmental criminology", su aparición en relación con la Chicago School of Sociology y su desarrollo en múltiples áreas, de entre las que destaca el "opportunity approach" para la explicación del evento criminal y, dentro de él, la TAC, véase el clarificador trabajo de BOTTOMS, A. E/ WILES, P.: "Environmental Criminology", en MAGUIRE, M./MORGAN R./REINER, R.:*The Oxford handbook of criminology,* Oxford University Press, 2ª ed, New york, 1997,pp. 305 y ss, y especialmente en lo que más nos interesa, pp. 320 y ss.

[47] CLARKE, R./FELSON, M.(EDS.): "Routine activity…", *ob. cit.*

No es tan extraño, pues, que la TAC, que también ve el delito como evento y que tiene una importante tendencia hacia la explicación preventiva, se utilice por los criminólogos de hoy para tratar de comprender un nuevo fenómeno como el cibercrimen.

En segundo lugar, no hay que desdeñar el hecho de que la TAC partiera, como una de sus premisas fundamentales, de la idea de que la modernidad, y en ella la evolución tecnológica[48], 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[49]. 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 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 éste 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. Una teoría, como la de las actividades cotidianas, que presta tanto atención a la relación entre cambio tecnológico y cambio del crimen, es especialmente adecuada para el análisis de si las TIC conllevan la creación de un ámbito de oportunidad criminal nuevo y distinto.

Al fin y al cabo, en tercer lugar y, a mi parecer, como razón que hace especialmente apta esta teoría (así como otras, como la de los estilos de vida) y en general todos aquellos enfoques del evento criminal, para el cibercrimen, las mismas centran la atención y el análisis en algo externo (aunque directamente relacionado con él cuando el evento sucede) al propio criminal, como es el propio lugar de comisión 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, si bien ello es perfectamente compatible con el análisis para cada delito en particular, de las teorías criminológicas que centran su atención en el agresor y sus condicionantes conducturales y cognitivos.

[48] De hecho, es de resaltar la importancia que otorga FELSON a la tecnología en la modificación de la criminalidad. Véase al respecto, especialmente, FELSON, M.: "Technology, Business and Crime", en FELSON M./CLARKE, R.V. (ED.):*Business and Crime Prevention,* New York, 1997, pp. 82 y ss., y más recientemente en FELSON, M,/BOBA, R.:*Crime and everiday life,* 4th edition, Sage, Thousand Oaks, CA, 2009, pp. 203 y ss.

[49] COHEN, L./FELSON, M.: "Social change…", *ob. cit.,* pp. 590 y ss.

Por último, e íntimamente relacionado con lo acabado de afirmar, un especial punto de unión entre el enfoque de la oportunidad y el cibercrimen, 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[50]. En efecto, y como advirtió Garland, las que él denomina "new criminologies of everydaylife", 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[51]. En palabras esta vez de Medina Ariza, "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"[52]. Es obvio que este enfoque tiene especial sentido ante un tipo de criminalidad como el que nos ocupa que, debido a que es realizada en el ciberespacio transnacional y anonimizado contra el que, de algún modo, van a chocar la Administración de Justiciay el Sistema penal nacional en general, requiere poner el foco de atención para su prevención, no sólo 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 puede servir para explicar que hayan sido varios los criminólogos anglosajones que, a partir de la TAC y de las teorías de la oportunidad, hayan planteado la posibilidad de que el ciberespacio sea un nuevo ámbito de riesgo criminal en el que se vean modificados algunos de los condicionantes relacionados con el delito[53]. Lo que no se ha hecho todavía, y este es el objetivo del trabajo y lo

[50] En el fondo esto tendría que ver con la segunda falacia del crimen, "the cops-and-courts fallacy", conforme a la cual se exagera la importancia de la policía, los tribunales y las prisiones como actores claves para la prevención del delito, mientras que debería recordarse que el crimen se produce antes y el sistema de justicia va después. FELSON, M,/BOBA, R.:*Crime and everyday…, ob. cit.*, p. 4.

[51] GARLAND, D.: *The Culture of Control. Crime and Social order in contemporary society,* Oxford University Press, New York, 2001, p. 128.

[52] MEDINA ARIZA, J. J.: "El control social del delito a través de la prevención situacional", en *Revista de Derecho penal y Criminología*, 2ª época, nº2, 1998, p. 281.

[53] En este sentido se manifiesta CAPELLER, quien después de señalar que algunas de las características de Internet, tales como la transnacionalidad, su fugacidad, la volatilidad de sus contenidos y las estrategias de los operadores en la comunidad virtual, tienen un impacto directo en materia penal, concluye que el impacto de dichos cambios en tal ámbito obliga, no sólo a una revisión del derecho sino también, de la teoría criminológica, que debería transitar hacia lo inmaterial para adaptarse al siglo XXI y evitar seguir "frente a un estado de caos virtual". CAPELLER, W.: "Notsuch a neat net...", *ob. cit.,* pp. 237 y ss., especialmente 240 y 241. Frente a ello es menos "tremendista" GRABOSKY (GRABOSKY, P.: "Virtual criminality...", *ob. cit,* p. 248), quien reconoce un cambio en el factor oportunidad (que él viene a identificar con el objetivo o víctima de la visión tradicional de la TAC), pero no en los sistemas de protección, ni en el autor motivado, respecto al cual señala, de forma muy gráfica que "si bien las tecnologías pueden cambiar rápidamente, no así la naturaleza humana. Los diez mandamientos son tan relevantes hoy como lo eran en tiempos bíblicos. La emoción del engaño que caracterizó la introducción del caballo de Troya, sigue vigente en la creación de sus descendientes digitales". Véase en sentido similar, en GRABOSKY, P./SMITH, R.: "Telecommunication fraud in the digital age: the convergence of technologies", en WALL, E. (ED.): *Crime and the Internet*, London, Routledge, 2001, p. 37; y de forma mucho más amplia, aunque con similares argumentos, en GRABOSKY, P.: "Computer crime: a criminological overview", en *Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Treatment of Offenders,* Vienna, 15 de abril de 2000. También analiza la cuestión PEASE, K.: "Crime futures and foresight: Challenging criminal behaviour in the information age", en WALL, D. (ED.): *Crime and the Internet*, *ob. cit.,* p. 23, que compara el *cyberspace* con el *meatspace*, señalando que mientras que en el último el número de víctimas está

será de futuras investigaciones teóricas y empíricas, es analizar cuáles son los cambios esenciales del evento criminal en el ciberespacio a partir de la extrapolación teórica de los elementos del crimen y, lo más importante, de la conjunción de los mismos, al nuevo ámbito en el que el mismo tiene lugar. Los caracteres intrínsecos y extrínsecos que, como hemos visto, configuran actualmente el ciberespacio y determinan todos los fenómenos que tengan lugar en él, anticipan que el cibercrimen, como evento social, será distinto al crimen en el espacio físico. No se está diciendo que las teorías que tratan de explicar el evento delictivo, como aquellas que tratan de comprender al criminal, no puedan hacerlo ahora con el cibercrimen, como tampoco, obviamente, que el crimen en Internet no sea un delito tal y como el mismo ha venido siendo discutido y definido por la criminología. Como indica el propio término, el cibercrimen es un crimen, un delito que debiera poder ser analizado y comprendido por cualquier teoría que trate de abarcar el fenómeno delictivo de forma completa o parcial. Lo que sucede es que tales parámetros, tales elementos definitorios del evento criminal, deben ser revisados con nuevos ojos al ser distinto el entorno o ámbito en el que se comete el delito[54]. El ciberespacio no cambia los caracteres esenciales que hacen que a determinados eventos se les pueda seguir denominando crímenes, pero sí modifica los parámetros espacio/tiempo en los que el crimen tiene lugar, por lo que es lógico que ello exija un replanteamiento, no tanto de las teorías criminológicas que tratan el crimen como evento, pero sí del propio evento y de los elementos del mismo con especial atención al contexto espacial y temporal en el que éste se produce.

2.2.2. ***El ciberespacio como un nuevo y "distinto" ámbito de oportunidad criminal***

La hipótesis de partida es que el cibercrimen, como evento criminal, también depende de la presencia de los elementos constitutivos de la ecuación del delito, un delincuente capacitado y motivado para el delito, un objetivo o víctima adecuado y la ausencia de un guardián capaz, en la primera fórmula de la TAC, así como de los demás elementos incorporados en las siguientes fórmulas[55], pero todos y cada uno

limitado por la velocidad en la que pueden situarse "frente al agresor", esto ya no ocurre en el ciberespacio donde muchas víctimas pueden ser dañadas a la vez. Precisamente PEASE ya había publicado un interesante trabajo sobre la evolución del crimen en el futuro en el que ya apuntaba algunos de los cambios criminológicos que podrían producirse en el ciberespacio, como por ejemplo, la diferente relación entre agresor y víctima, fruto de la inexistencia de un contacto visual directo de uno con otra, DAVIES, R./PEASE, K.: "Crime, technology and thefuture", en *SJ*, núm. 13, abril, 2000, p. 61. Algunas de estas y otras referencias son apuntadas por YAR, M.: "Thenovelty of 'cybercrime':...", *ob. cit.,* pp. 407-427, quien, a mi parecer, realiza el análisis más completo sobre la validez de los tópicos de la criminología clásica para la comprensión de unos crímenes aparentemente nuevos como los cometidos en el ciberespacio.

[54] En idéntico sentido, YUCEDAL, B.: "Victimization in…., *ob. cit*., p. 43.

[55] A los tradicionales elementos se pretendió añadir posteriormente un cuarto elemento, la ausencia de una persona que controle las actividades del ofensor motivado (*personal handler*), y después el gestor del lugar. FELSON, M.: "Linking criminal choices, routine activities, informal control and criminal outcomes", en CORNISH, D.B./CLARKE, R. V. (EDS.): *The reasoning Criminal, Rational choice perspectives on offending*, Springer-Verlag, New York, 1986. Véase también sobre ello ADLER, F./MUELLER, G. O. W./LAUFER, W. S.:*Criminology and the Criminal Justice System*, McGraw Hill, New York, 4th edition, 2001, p. 241, y también TILLEY, N.: *Crime prevention.,ob. cit.,* p. 120. Así, los tres elemen-

de estos elementos se ven modificados en algún sentido al darse en el ciberespacio. No de una forma tal que cambie su esencia, pero sí de modo que la confluencia de los mismos en el evento resulta distinta a la que define al crimen en el espacio físico.

Se trata, por tanto, de contrastar los elementos del delito con los caracteres intrínsecos y extrínsecos del ciberespacio, para definir 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. Voy a hacerlo de forma separada, dividiendo el análisis entre 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, al lugar (que es el propio ciberespacio). Ello no significa que crea que se trate de elementos separados: a mi parecer la TAC aporta la idea de que para la comprensión del delito no sólo hay que mirar al agresor, sino también otros elementos del evento, pero es obvio que todos los que lo conforman están interrelacionados, de modo tal que la propia motivación del agresor depende de los demás factores, así como el objetivo es definido como adecuado por la conducta del agresor, etc. El estudio separado de los elementos es, por tanto, meramente a efectos didácticos. El cibercrimen, como el delito en el espacio físico, es la confluencia de las partes en el todo.

2.2.2.1. *El ciberagresor motivado*

Los caracteres intrínsecos del ciberespacio, su propia esencia como ámbito virtual en el que las coordenadas ya no son definidas en términos de distancia, sino, más bien, de posibilidades de comunicación, producen como primer efecto de mutación del ámbito de oportunidad criminal, el incremento significativo de los márgenes potenciales del evento criminal. Al no existir distancias que actúen como barreras y dificulten el contacto entre las personas y sus bienes, entre los agentes motivados y los objetivos adecuados, el potencial número de los que pueden acabar siendo unos y otros, aumenta. Al fin y al cabo, y como han señalado Brenner y Clarke, en el mundo real (físico), el autor y la víctima generalmente están próximos, en términos de distancia física, cuando se produce el delito: no sólo no es posible la violación o el homicidio si agresor y víctima no están juntos en el momento del ataque, sino que gran parte de los fraudes se producen debido a que ha existido un contacto, hasta el punto de que en un mundo no tecnológico no es

tos que conformaban el delito en un primer momento, agresor, objetivo y ausencia de guardián, mutaron primero en la sustitución del guardián por el lugar en el primer triángulo, y después con la incorporación de un segundo triángulo superpuesto al primero en el que el guardián capaz tutela el objetivo adecuado, el *personal handler* al agresor motivado y el gestor del lugar al espacio en el que se produce el ataque.

posible robar o defraudar la propiedad si el ladrón y la víctima se encuentran en diferentes países o ciudades[56]. Desde hace tiempo algunas tecnologías posibilitan que esto no sea así, pero 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[57], por lo que el ciberespacio se constituye 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[58], expandiéndose, por tanto, el ámbito potencial de oportunidad criminal[59].

En última instancia se trata, por tanto, de que Internet elimina la exigencia de proximidad entre agresor y víctima para la existencia de un delito[60], con todo lo que ello supone desde una perspectiva preventiva, pero también para la investigación del crimen y el posterior enjuiciamiento del mismo. Mientras que lo usual en la criminalidad suele ser que el delincuente realice el delito cerca de su propia residencia[61], 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 a cientos o miles de kilómetros de distancia[62]. Es obvio que la no necesidad del desplazamiento físico representa una reducción del coste de ejecución del delito al que se sumarán otros, como la dificultad para ser identificado y "cazado" o, en algunos casos, la reducción de la conciencia de ilicitud y la minimización de la desmotivación que puede devenir de la percepción de legitimidad de la norma que prohíbe su comportamiento.

Por otra parte, las TIC actúan en la actualidad como un "multiplicador de fuerza"[63] que hace que personas con mínimos recursos puedan generar grandes daños para múltiples personas y bienes en el ciberespacio[64]. 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. Me explico. 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

[56] BRENNER, S. W Y CLARKE, L. L.: "Distributed Security: preventing cybercrime", en *TJMJCIL,* Summer 2005, pág. 3.

[57] Así señalan ADLER, F./MUELLER, G. O. W./LAUFER, W. S.:*Criminology and the Criminal…, ob. cit.,* p. 351, que en el ciberespacio, los movimientos físicos son reemplazados por los "viajes electrónicos", por lo que los agresores ya no necesitan estar al lado de las víctimas.

[58] JONES, B. R.: "Comment: virtual neighborhood watch: open source software and community", en*Journal of Criminal Law & Criminology,* vol. 97, núm. 2, winter, 2007, p. 610.

[59] En este sentido también, MCQUADE, S. C.: "Cybercrime", en TONRY, M (ED.).:*The Oxford Handbook of Crime and public policy,* Oxford University Press, New York, 2009,p. 481.

[60] JONES, B. R.: "Comment: virtual…, *ob. cit.*, pp. 610 y ss.

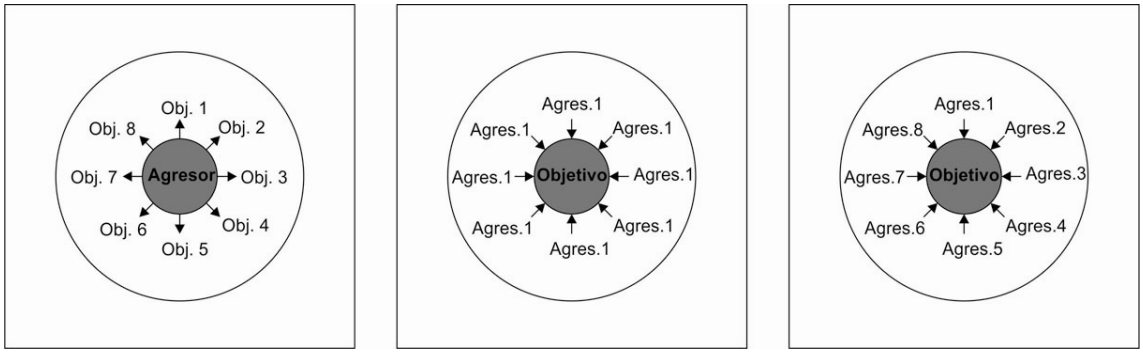
[61] BOTTOMS, A. E/ WILES, P.: "Environmental Criminology", *ob. cit.,* p. 323.

[62] KSHETRI, N.: "The Simple Economics of Cybercrimes", en *IEEE Security & Privacy,* The Ieee Computer Society, 2006, en Internet en http://see.xidian.edu.cn/hujianwei/papers/098TheSimpleEconomicsofCybercrimes.pdf

[63] YAR, M.: "The novelty of 'cybercrime'…", *ob. cit.,* p. 411.

[64] También, PEASE, K.: "Crimefutures…", *ob. cit.,* p. 23

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 serie de gráficos 4, 5 y 6, los agresores pueden seleccionar entre múltiples objetivos a atacar sin que haya que recorrer distancia, por lo que de forma sinalagmática, una misma víctima puede ser atacada por múltiples agresores; pero, además, 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[65].



Gráficos 4, 5 y 6. **Dinámicas de los ciberataques:** Es posible tanto que un agresor actúe a la vez sobre varios objetivos (4), que actúe contra un objetivo desde varios lugares en el ciberespacio como en los DDoS con bots (5), como que varios agresores ataquen simultáneamente a un mismo objetivo como en los DDoS (6)

Y lo más significativo es que, frente a la criminalidad en el espacio físico, el ataque se pude hacer desde cualquier parte del mundo[66].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[67], 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

[65] MCQUADE, S. C.: "Cybercrime", *ob. cit.,* p. 482.

[66] PEASE, K.: "***Science in the service of crime reduction"***, en TILLEY, N. (ED.): *Handbook of crime prevention and community safety,* Willan Publishing, UK, 2005, p. 181.

[67] HUTCHINGS, A./HAYES, H.: "Routine Activity Theory...", *ob. cit.,* p. 435.

con el consiguiente potencial aumento de la criminalidad[68]. 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[69].

Además, el ciberespacio no sólo 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.

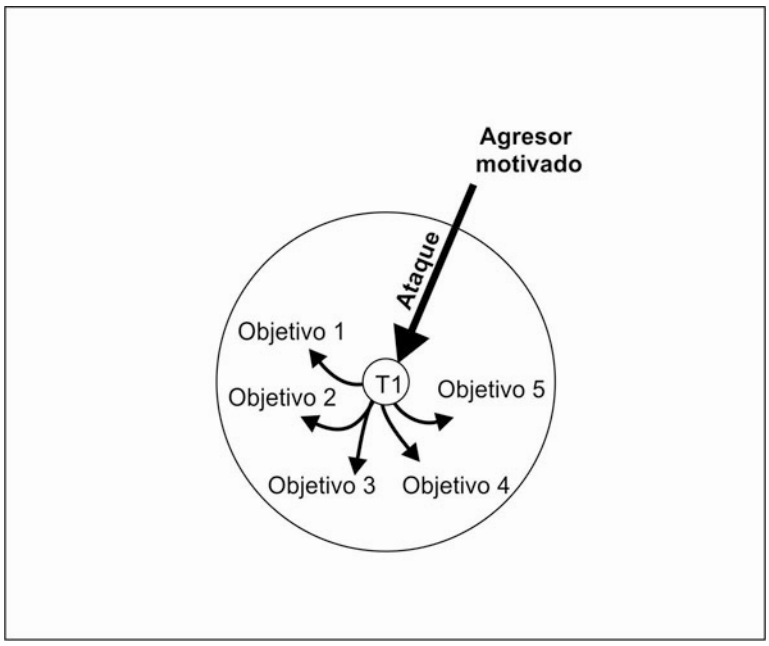


Gráfico 7. **Ataque múltiple**: Con la misma acción se atacan diversos objetivos (y en el mismo tiempo)

Y todos estos ataques a uno o varios objetivos pueden realizarse en el mismo tiempo, 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 cibera-

[68] En el mismo sentido, entre otros, GRABOSKY, P.: "Virtual Criminality...",*ob. cit.,* p. 248, y NISBETT, C.: "New directions on Cybercrime", White Paper, Qinetiq, en Internet en http://apps.qinetiq.com /perspectives/pdf/EP_White_Paper3_Cyber%20Crime.pdf , p. 2.

[69] CLOUGH, J.: *Principles of Cybercrime, ob. cit.,* p. 5.

taques 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. A esto es a lo que, a mi parecer, se refiere Alshalan cuando señala que en el ciberespacio puede desaparecer el agresor motivado de la ecuación del delito en el caso de los ataques con virus[70]. 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 éste como de la de la víctima. Esto ocurre especialmente en el caso de los virus que son descargados en una determinada página web de descarga 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.

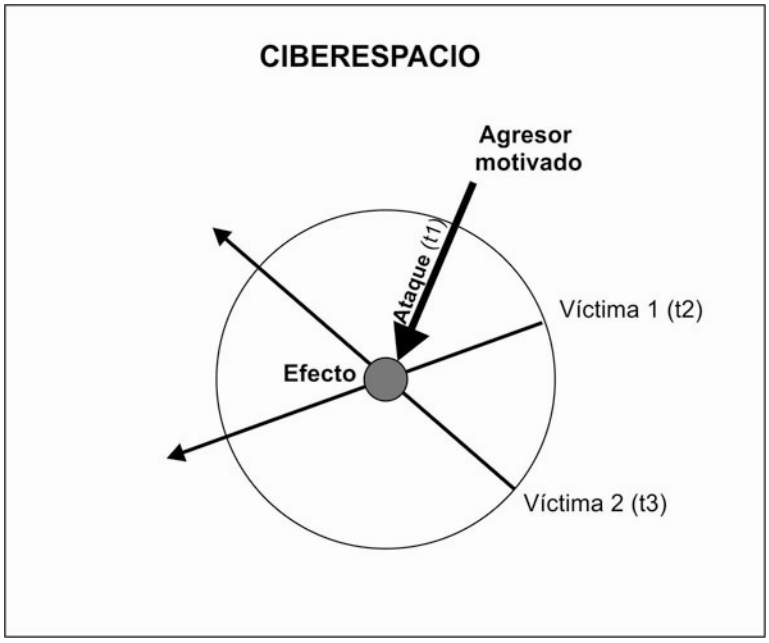


Gráfico 8. **Fijación del ataque e interacción de la víctima:** El ataque deja un efecto fijo en el ciberespacio, siendo la víctima la que interacciona con él.

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

[70] ALSHALAN, A.: *Cyber-Crime Fear and Victimization: An Analysis of A National Survey,* Mississippi State University, 2006, p. 146, al señalar que "*In cyberspace, the place is the Internet, and time eventually provides a virus or a spy-ware, and the crime does not require an offender to be present*".

víctima-receptor 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[71]. 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.

Gráficos 9 y 10. **La víctima como instrumento de difusión del ataque.** En el 9 la víctima difunde el ataque a sus contactos, en el 10 son las víctimas las que, al interaccionar con ella, se infectan.

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[72], lo cual, a su vez, le permite reinventarse y adoptar nuevos personajes virtuales con los que, quizás, cometer delitos[73]. Con el anonimato ocurre, por tanto, algo muy similar a lo que relatábamos en relación

[71] También reconoce la multiplicación de los efectos de los ataques en el ciberespacio AGUSTINA SANLLEHÍ, J.R.: "La arquitectura digital de Internet como factor criminógeno", en *International e-Journal of Criminal Science,* art. 4, núm. 3, 2009, p. 9.

[72] PITTARO, M. L.: "Cyber stalking...",*ob. cit.,* p. 181.

[73] YAR, M.: "The novelty of 'cybercrime'...", *ob. cit.,* p. 421.

con la transnacionalidad, que incide en la desaparición del temor a ser identificado y en la consiguiente minimización del temor a ser detenido[74], frenos de la motivación criminal que le convierten en un "motivated offender"[75]. 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 cibercirminal[76]. Porque no sólo 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[77]. De momento, sin embargo, ello no parece posible, pues el anonimato no sólo 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.

2.2.2.2. *Objetivos adecuados en el ciberespacio: del VIVA al IVI*

Hasta el momento, hemos centrado nuestra atención sobre el posible cambio que Internet conlleva en el ámbito de riesgo criminal en la interacción entre algunos de los factores intrínsecos y extrínsecos de Internet con el factor agresor motivado. Sólo indirectamente, al venir concatenado el ataque del agresor con la víctima que lo recibe, nos hemos fijado en el "objetivo adecuado", especialmente al afirmar que Internet aumenta el número de agresores potenciales que pueden coincidir con las víctimas en un espacio determinado, y al destacar que el éxito del ataque del agresor motivado puede depender de que la víctima interaccione con el mismo que esté fijo en el ciberespacio esperando a ser "encontrado" por el objetivo. Los "suitable Targets" por tanto, no tienen que encontrarse a una distancia cercana al agresor para serlo, sino que pueden convertirse en víctima, objetivos situados en el mismo ciberespacio aunque a miles de kilómetros de distancia.

Esto confirmaría el que era, como ya se dijo, uno de los presupuestos teóricos de la TAC: que el aumento del contacto entre las personas, derivado del desarrollo tecnológico, explicaba en parte el aumento de la criminalidad en las últimas déca-

[74] También en este sentido, MESTRE DELGADO cita como una de las tres leyes del cibercrimen, la ocultación de los autores "por los anchos dominios de la aldea global", junto con la optimización de la eficacia del esfuerzo criminal y la minimización de los riesgos para al agresor derivados de la relación personal con la víctima. MESTRE DELGADO, E.: "Tiempos de cibercrimen", en *LL,* núm. 37, año IV, abril, 2007, p. 3.

[75] PITTARO, M. L.: "Cyber stalking...",*ob. cit.,* p. 181.

[76] PITTARO, M. L.: "Cyber stalking...",*ob. cit.,* p. 189.

[77] LONGE, O. B./MBARIKA, V./KOUROUMA, M./WADA, F./ISABALIJA, R.: "Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities", en *IJCSIS,* vol. 6, núm. 3, 2009, p. 127.

das[78]. Pero, obviamente, ese tipo de contacto difiere en cuanto a su naturaleza del contacto, potencialmente mayor en lo cuantitativo, pero quizás menor en lo cualitativo, por excluir el ámbito físico, que puede tener lugar entre las personas en el ciberespacio. Y esta es, a mi parecer, una de las importantes precisiones que deben hacerse a la idea del aumento potencial del contacto entre agresores y objetivos pero, a la vez, el punto de inicio argumental desde el que definir las condiciones que pueden hacer adecuado a un objetivo en el ciberespacio. Me explico a continuación desarrollando con más profundidad la idea:

El contacto entre víctima 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.

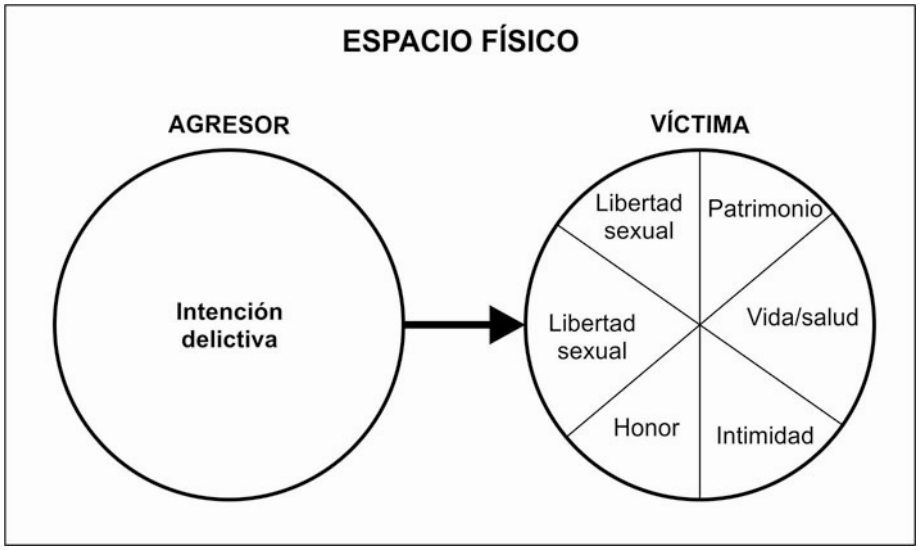


Gráfico 11. **Contacto en el espacio físico.** Agresor contacta con la víctima (con todos sus bienes) y selecciona los bienes a los que quiere afectar de todos los que posee.

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

[78] COHEN, L./FELSON, M.: "Social change…", *ob. cit.*, pp. 565 y ss.

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 (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), 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 demás, situar tales bienes en ese ámbito de riesgo nuevo.

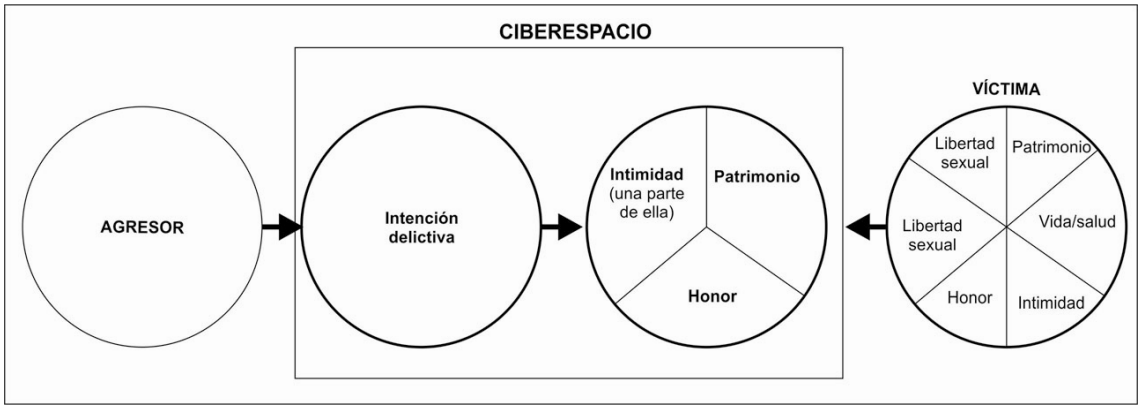


Gráfico 12. **Contacto en el ciberespacio**. La víctima no entra en toda su integridad en el ciberespacio, sino que lo hace con algunos bienes, y son esos, los que pueden ser atacados según la intención del agresor

Los usuarios del ciberespacio pueden, por tanto, eliminar del ámbito de ataque aquellos bienes que no incorporen al ciberespacio. Apoyándonos en uno de los elementos del acrónimo CRAVED, utilizado por Clarke para definir los bienes preferidos por los ladrones (*Concealable, Removable, Available, Valuable, Enjoyable and Disposable*)[79], podríamos decir que si una víctima no introduce un bien en el ciberespacio, el mismo no estará disponible (*not Available*) y no podrá ser objeto del ataque. 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 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, por ejemplo, podríamos citar los estudios empíricos que demuestran la relación entre la entrega de información personal *on*

[79] CLARKE, R. V.: "Hot products: understanding, anticipating and reducing demand for stolen goods", Paper nº 112, Police Research Series, British home Office Research Publications, London, 1999.

line y la victimización por los delitos más relacionados con los jóvenes como víctimas como el *cyberbullying* y el ciberacoso sexual a menores[80]. En este último caso, hay estudios que constatan 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[81]. 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 victimizacion. En efecto, los estudios victimológicos existentes sobre el *on line grooming* parecen demostrar que mientras que el mero hecho de colgar información personal en páginas web o redes sociales[82], no es un factor que incide en el aumento de riesgo de recibir un ataque de *grooming,* sí lo es el enviar directamente información personal a desconocidos.

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[83], 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[84]. La diferencia estriba en que previamente a todo ello, la introducción del objeto, por parte de la propia víctima,

[80] Así, además de los citados, el de MARCUM, CATHERINE D.: "Adolescent online victimization and Constructs of Routine Activities theory", en JAISHANKAR, K (ED.):*Cyber Criminology. Exploring Internet crimes and criminal behavior,* CRC Press, Boca Ratón, 2011, p. 269.

[81] WOLAK, J./FINKELHOR, D. /MITCHELL, K. J./YBARRA, M. L.: "Online "Predators" and their Victims: Myths, Realities and Implications for Prevention and Treatment", en *American Psychologist,* vol. 63, núm. 2, 2008, p. 112.

[82] WOLAK, J./FINKELHOR, D./MITCHELL, K. J./YBARRA, M. L.: "Online "Predators"... *", ob. cit.,* p. 114.

[83] Correspondientes a *Value of crime target, the Inertia of crime target, the physical visibility of crime target, accessibility of crime target* (VIVA). FELSON, M.: *Crime and everyday life,* 2nd edition, Thousand Oaks, CA: PineForge Press, 1998, pp. 54 y ss.

[84] Esto lo ha hecho con profundidad, aunque a mi parecer no con total acierto, YAR, M.: "The novelty of 'cybercrime'...", *ob. cit.,* pp. 419 y ss. Posteriormente también relaciona el VIVA con los objetivos del ciberespacio CHOI, K.: "ComputerCrime…", *ob. cit.*, p. 312.

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? Trataré a continuación de analizar cada uno de ellos para, en el caso de que los mismos no sean suficientemente expresivos y definitorios de la distinta capacidad de adecuación de los objetivos, sustituir el acrónimo VIVA por otro más adecuado al nuevo ámbito de intercomunicación social en el que se puede producir el delito.

Pues bien, el primer elemento a 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 por sí mismo 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[85], y esto será igual en el ciberespacio: las 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[86]. 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. Yar ha tratado de mantener el elemento al considerar que lo anterior no implica que no haya inercia de los bienes en el ciberespacio, pues una reflexión más profunda muestra que incluso la información conserva las propiedades de inercia en algún grado, en relación, por ejemplo, con el volumen de los datos (cuanto mayor sea, mayor es la dificultad de la descarga) o el sistema informático utilizado[87]. A mi parecer, el intento de Yar es vano. La evolución actual de las TIC contradice lo por él afirmado, y salvo en singulares casos excepcionales, los bienes en el ciberespacio apenas se diferenciarán entre sí por sus mayores o menores condiciones intrínsecas (y no relacionadas con los

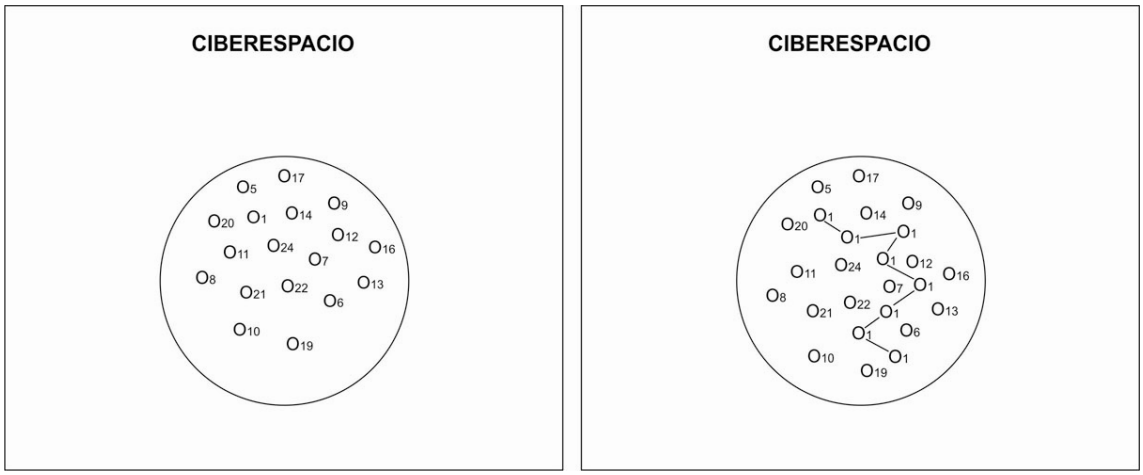
[85] FELSON, M.: *Crime and..., ob. cit.,* p. 55.
[86] FELSON, M.: *Crime and..., ob. cit.,* pp. 55 y 56.
[87] YAR, M.: "The novelty of 'cybercrime'...", *ob. cit.,* p. 420.

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[88]. 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, como ha señalado Yar, observación del delincuente por medio de sistemas de rastreo o de señalización[89], pero eso no convierte al objetivo en menos adecuado, sino al gestor del lugar (o al guardián si deviene de la propia víctima el sistema e impide el ataque) en más eficaz. 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[90]. Señala Yar que es esencia del ciberespacio su carácter público, por lo que todo en él está visible a nivel mundial[91]. A mi parecer, esto sólo es así parcialmente. Es indudable que la entrada en el ciberespacio conlleva la irrupción en un espacio público, pero eso no significa que se sea "visible", pues puede ocurrir que alguien acceda a Internet y nadie, excepto quienes le proveen el acceso, se aperciba de ello. El ciberespacio es tan ingente y tan universal, que más bien 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. Hay algo, sin embargo, que hace visibles a los sujetos en el ciberespacio, su interacción con otros sujetos y con otros servicios. La interactividad sí es la esencia de Internet, y a mayor interacción con otros agentes, con diferentes páginas web, con variados servicios, mayor posibilidad de ser percibido (ser visible) por parte de otros.

88 FELSON, M.: *Crime and..., ob. cit.,* p. 58.
89 YAR, M.: "The novelty of 'cybercrime'...", *ob. cit.,* p. 421.
90 FELSON, M.: *Crime and..., ob. cit.,* p. 56.
91 YAR, M.: "The novelty of 'cybercrime'...", *ob. cit.,* p. 420.



Gráficos 13 y 14. **Visualización de objetivos en el ciberespacio e interacción.**
Los objetivos se diluyen en el ciberespacio (13), pero el objetivo 1 se hace más visible cuando interacciona y se mueve por Internet (14).

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[92] 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*[93], 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, por medio de este estudio empírico de regresiones logísticas Alshalan 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[94] y, exclusivamente para la infección por virus, con el hecho de el tener hijos que acceden al ciberespacio[95]. Por su parte, Yucedal, quien examina los factores que inciden en la victimización por conductas de *spyware* y *adware* a partir de los presupuestos de las citadas teorías, 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

92 ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* p. 123.
93 ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* pp. 47 y ss.
94 ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* p. 126.
95 En efecto, tener hijos resulta un factor determinante del riesgo de victimización por infección de virus, pero no para el resto de la cibercriminalidad. ALSHALAN, A.: *Cyber-CrimeFear..., ob. cit.,* p. 127, plantea dos posibles explicaciones al fenómeno: la primera, que los niños desconozcan las amenazas potenciales de algunos sitios web y, por eso, se descarguen archivos con virus. La segunda, apoyada por la TAC, sería que cuando los encuestados contestan que tienen niños con acceso a Internet, quieren decir que lo utilizan, por lo que la frecuencia y duración de la utilización de Internet aumentaría. Quizás sea en realidad una mezcla de ambas: los menores utilizan Internet y, además, realizan muchas más actividades en el ciberespacio que los adultos. En todo caso, todas las explicaciones certificarían la tesis de que a mayor interacción en el ciberespacio, mayor adecuación del objetivo.

propio sujeto el que al visitar una determinada web o al descargarse un programa, cargue involuntariamente el virus[96]. 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 TAC[97]. También por medio de un estudio empírico de ecuaciones estructurales para la evaluación de la relevancia de variables como el estilo de vida en Internet y la utilización de sistemas informáticos de protección, Choi 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[98].

Y esto es así con otro tipo de cibercrímenes. Así, 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[99], y ya hemos visto anteriormente que también había una intensa relación entre la interacción de la víctima en chats y demás con la victimizacion por on line grooming o delitos similares.

En el ciberespacio, por tanto, a mayor interacción de un sujeto, plasmada en mayor tiempo en línea o mayor variedad de actividades en Internet (descarga de archivos, entrada en plataformas p2p, realización de compras en línea, creación de perfiles en redes sociales, etc.), 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 sólo con la interacción se producirá el contacto (necesario para el delito) en el vasto ciberespacio entre el agresor motivado y la víctima, dependiendo también de que esta "se mueva" por Internet el que el mismo se produzca, 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.

Podemos concluir, pues, que las condiciones para la adecuación del objetivo del crimen VIVA no son transportables al ciberespacio[100], excepto en el caso del Valor.

[96] La medición del estilo de vida como determinante del riesgo de victimización lo realiza YUCEDAL a partir de un modelo de medida de dos factores consistentes en la realización de actividades *online* básicas o de ocio. En las actividades básicas se incluyen comportamientos relativamente seguros (en relación con la infección por *adware* o *spyware*) realizados en Internet, tales como la lectura de correos electrónicos, crear o leer *blogs*, o la compra *online*; mientras que en las actividades *on line* de ocio se incluyen conductas más peligrosas, como la descarga de música, de vídeos o de programas que pueden contener software de este tipo o el juego *on line.*YUCEDAL, B.: "Victimization in…", *ob. cit.,* pp. 113 y ss.

[97] CHOI, K.: "ComputerCrime…", *ob. cit.*

[98] CHOI, K.: "ComputerCrime…", *ob. cit.*, p. 321. Frente a la forma de medición de YUCEDAL, la variable del estilo de vida *on line* es medida por medio de tres variables distintas, actividades vocacionales y de ocio, actividades de ocio peligrosas, y actividades vocacionales de riesgo.

[99] YBARRA, M. L./MITCHELL, K.: "Exposure to Internet Pornography among Children and Adolescents: A National Survey", en *Cyberpsychology& Behavior,* vol. 8, núm. 5, 2005, pp. 473 y ss.

[100] Lo admite, aunque mucho más tenuemente, y tratando finalmente de incorporar las condiciones a la ecuación, YAR, al no poder sino reconocer que las variables inercia, visualización y accesibilidad "presentan una considerable

Éste 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: que el bien o la persona haya sido **Introducido** en el ciberespacio; que tenga un **Valor** que lo haga apetecible para el cibercriminal; y 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. Es hora de analizar otros factores del evento criminal en el ciberespacio.

2.2.2.3. *Guardianes capaces y gestores del lugar "ciberespacio"*

No podemos finalizar esta abstracción teórica para la revisión del crimen en el nuevo ámbito de oportunidad criminal que es el ciberespacio sin analizar la incidencia del mismo, con sus caracteres intrínsecos y extrínsecos, con el otro factor de la ecuación del delito conforme a la definición de la TAC de Cohen y Felson. Me refiero a la ausencia del guardián capaz, sin la cual no hay delito, y que en el ciberespacio también ve ampliado sus límites, esto es, disminuye la capacidad potencial del guardián de evitar el crimen. 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. En otros términos, la transnacionalidad puede incidir en una disminución de la eficacia de los elementos de protección de la víctima frente al ofensor capaz y dispuesto, con el consiguiente riesgo de victimización que supone la inexistencia de mecanismos de tutela[101], y al mismo tiempo, puede ayudar a que el criminal se motive hacia la comisión del delito al percibir como compleja y alejada su identificación, la persecución judicial del mismo y los efectos negativos que de ello se derivarían[102].

Como señalaron Farrell y Pease, la noción de Guardián Capaz se convierte en importante, pero también compleja, cuando pensamos en el cibercrimen[103]. Quizás en este sentido, sea más útil la diferenciación entre el mánager o gestor del lugar, y

divergencia entre su valor en el mundo real y el virtual". YAR, M.: "The novelty of 'cybercrime'...", *ob. cit.*

[101] También destacan la relación entre la victimización en el cibercrimen y la ausencia de un "capable guardian" físico, GRABOSKY, P./SMITH, R.: "Telecommunication fraud…", *ob. cit.* p. 37, aunque más que referirse a los medios institucionales, se refieren a los sistemas de protección físicos, tales como antivirus, etc.

[102] En sentido similar, no refiriéndose específicamente a la transnacionalidad, pero sí a la dificultad de identificación de los criminales en Internet y a la posibilidad de que ello motive la realización de cibercrímenes, YAR, M.: "The novelty of 'cybercrime'…", *ob. cit.,* pp. 407-427.

[103] FARRELL, G./PEASE, K.: "Criminology and Security", en GILL, M (ED.):*The Handbook of Security,* Perpetuity Press, 2005.

el guardián que opera directamente sobre la víctima o el objetivo potencial, conforme a la segunda versión del triángulo del delito. 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[104]. 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, en el triángulo del delito, los guardianes de los objetivos adecuados. Éstos 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. Como han señalado Bossler y Holt, 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[105].

Los estudios empíricos demuestran que tales sistemas pueden ser muy eficaces para evitar la victimización por el cibercrimen. Así, Yucedal constata que el uso de instrumentos digitales de seguridad, tales como cortafuegos, antivirus o programas *anti-spyware* como guardianes capaces, determina el riesgo de victimización[106], y a las mismas conclusiones llega Choi respecto al que él considera elemento esencial de la TAC[107].

Pero se trata, en todo caso, y a mi parecer, 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.)[108], pero no "parte de ella", como sí lo es el software que la víctima no pone en su ordenador. En el caso del ciberes-

[104] Así, también, YAR, M.: "The novelty of 'cybercrime'…", *ob. cit.,* pp. 407-427.
[105] HOLT, T. J/BOSSLER, A. M.: "On-line Activities…",*ob. cit.*
[106] YUCEDAL, B.: "Victimization in…", *ob. cit.,* pp. 117 y ss. En el caso de la incorporación de sistemas de autoprotección, el estudio utiliza como variables la tenencia de cortafuegos y de antivirus.
[107] CHOI, K.: "ComputerCrime…", *ob. cit.*, p. 321.
[108] COHEN, L./FELSON, M.: "Social change…", *ob. cit.,* p. 590; y también FELSON, M.: *Crime and..., ob. cit.*, p. 53.

pacio es la propia víctima, por tanto, el propio objetivo, el que debe incorporar sus guardianes capaces.

Lo relevante, en todo caso, no es situar los antivirus, cortafuegos y demás en el lado del triángulo del objetivo adecuado o de la ausencia de guardián capaz, sino reconocer que en la conjunción de estos elementos, y por tanto, en la propia prevención del delito, la víctima juega un papel preponderante en el caso del cibercrimen, dado que de ella depende en parte, no sólo su adecuación como objetivo (las dos ies, Introducción e Interacción), sino también su propia autoprotección, pues será ella la que defina los guardianes capaces que la protegerán al tener sistemas antivirus, al actualizarlos, al incorporar otros sistemas de detección de software de riesgo, al actualizar el sistema siempre que se pueda, etc. El guardián capaz, en el ciberespacio, es prácticamente un autoguardián que depende de la propia víctima.

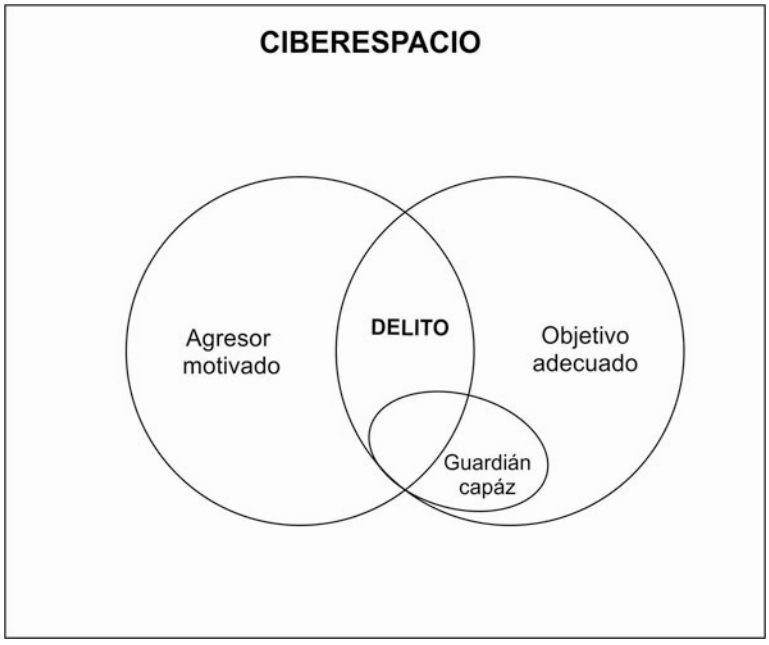


Gráfico 15. **Triángulo del cibercrimen.** El guardián capaz depende del propio objetivo, pues apenas hay guardianes externos, por lo que el efecto reductor del delito es menor.

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, como ha señalado Grabosky, exige una intervención y esfuerzo plural de instituciones y usuarios[109]. En todo caso esto parece

[109] GRABOSKY, P.: "Virtual Criminality: ...",*ob. cit.,*p. 248.

más lejano. Ante la inexistencia actual de formas de control formal más institucionalizadas, 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[110].

Por último, merece la pena destacar que el hecho de que las TIC estén en constante evolución y que los usos sociales y comerciales del ciberespacio, vigentes hoy, no tengan porqué ser los del mañana, también tiene consecuencias en términos de oportunidad delictiva, muy especialmente en relación con la "capacidad" del agresor y en la "incapacidad" del guardián y de la propia víctima para asegurar su propia defensa. Así, la evolución permanente del ciberespacio, de sus tecnologías y sus servicios, complica la eficacia de los protectores que son capaces para los riesgos que conocen, pero no para los nuevos, y tanto en relación con la aparición de nuevos medios de ataque a objetivos adecuados tradicionales, como en el propio surgimiento de nuevas oportunidades correspondientes a nuevos bienes aparecidos a la luz de las nuevas relaciones sociales en el ciberespacio. En cuanto a lo primero, es obvio que la rapidez con la que evoluciona la tecnología hace enormemente compleja la eficacia de los mecanismos de control y protección de los intereses socialmente esenciales. La actualización de los instrumentos y herramientas de los criminales va a ser aún mayor en el ciberespacio que en la criminalidad física que, de hecho, está aprovechándose ya de las TIC para mejorar en eficacia y eficiencia. Además, el carácter abierto del ciberespacio, el hecho de que sean los propios usuarios los que puedan hacer evolucionar el mismo, conlleva la posibilidad, para los que tengan grandes conocimientos informáticos, de cambiar protocolos y usos para su propio interés que, también, puede ser criminal. Por otra parte, y en segundo lugar, esta misma mutación constante de las TIC y de la interacción social con las mismas, conlleva la aparición de nuevos intereses sociales o de nuevas dimensiones de valor de los existentes que, precisamente por no existir o no expresarse de la forma en que lo hacen ahora previamente, tampoco pueden ser convenientemente protegidos.

3. **CONCLUSIONES Y REFLEXIONES PARA EL FUTURO**

3.1. **¿Hacia el aumento de la criminalidad en Internet? El cibercrimen y el "efecto iceberg"**

El anterior análisis nos deja muchas ideas que debieran ser desarrolladas, lo cual no será posible hacerlo aquí con la profundidad necesaria. Una de las conclusiones que, sin embargo, se adivinan más claras es la que se refiere a que los márgenes del ámbito de oportunidad criminal dependientes del agresor motivado y de su relación

[110] GRABOSKY, P.: "Virtual Criminality: ...",*ob. cit.,*p. 248.

con la víctima u objetivo potencial aumentan en el ciberespacio al eliminarse el efecto distancia física, siendo mucho más amplio el abanico de contacto criminal potencial existente y no limitándose ni a lo espacial ni a lo temporalmente cercano[111]. Es decir, que el uso de Internet aumentaría la capacidad de un agresor motivado de atacar a una víctima en ausencia de un guardián capaz, al reducirse el efecto de la distancia física como condicionante del evento criminal. En otras palabras, el ámbito de oportunidad criminal aumenta. Obviamente tal afirmación no incluye otras como que la delincuencia, en sentido macro o global, aumentará, ni aquella otra posible relativa a que la delincuencia en el ciberespacio acabará por ser mayor que la realizada en el espacio físico. Pero, en cambio, sí conlleva la afirmación de que conforme las TIC vayan avanzando y la vida diaria de las personas se vaya desarrollando en el ciberespacio, aumentando los bienes que son puestos en el mismo, incrementándose el valor de la información, y ampliándose las formas de interacción social en Internet, la delincuencia en Internet aumentará y no será, como parece ahora, testimonial sino que tendrá cada vez mayor importancia. Si ello supondrá una desviación parcial del crimen del espacio físico al ciberespacio o una duplicación (también parcial) de la criminalidad en dos ámbitos distintos, es una cuestión compleja que requeriría de un análisis mucho más profundo imposible aquí.

En todo caso debe matizarse la afirmación o, más bien, deben tomarse en cuenta factores que pueden debilitar, si bien no impedir, el alcance del incremento potencial del crimen en el ciberespacio. El primero de ellos es que el crecimiento potencial se limita a las infracciones que no requieren contacto físico directo, lo cual, a su vez, restringe enormemente el número de bienes que pueden ser afectados y conllevará que la cibercriminalidad difícilmente pueda llegar a equipararse cuantitativa y cualitativamente a la realizada en el espacio físico. Como se ha avanzado anteriormente, debido a la especial naturaleza virtual o no-física de la comunicación en el ciberespacio, los bienes directamente relacionados con las personas, especialmente con su salud física, difícilmente podrán ser puestos en riesgo por medio de un ciberataque. Para matar o lesionar aún es necesario el contacto directo (físico) entre agresor y víctima o, cuanto menos, entre el arma empleada por el agresor y su objetivo potencial, lo cual hace que aún sea sólo en la ficción posible, el asesinato por medio de Internet. Y no son la salud y la vida los únicos bienes a salvo del ciberespacio, sino también otros bienes colectivos, si bien indirectamente relacionados con ellos, como los delitos contra la seguridad vial, de tráfico de drogas, delitos ambientales, fraudes alimentarios, de manipulación genética, etc.[112].

[111] En el mismo sentido se manifiesta YUCEDAL, B.: "Victimization in…",*ob. cit.,* p. 43, señalando que "cyberspace can be considered as an expansive neighborhood on a global scale. We can argue that every time a person connects to the Internet, he or she spends time in the higher crime rate area just like in the physical world, and that makes him or her potential target".

[112] No parece tan descabellado ya, sin embargo, la realización remota a través de redes telemáticas de algunos de estos delitos, por ejemplo, en el caso de la manipulación genética o de los fraudes alimentarios en los casos de que el

Otros bienes como el patrimonio o la libertad sexual, pueden ser atacados en el ciberespacio, pero no de determinadas formas que, al ser de carácter físico y estar tipificadas expresamente, excluyen la posibilidad de la realización de determinados delitos en el ciberespacio. Es el caso de la violación o de concretas formas de abuso sexual que exijan un contacto físico, y del hurto o el robo con violencia (con lesiones o con homicidio, tal y como se regula en otros países), y de muchos otros tipos penales como los delitos societarios, etc. Por decirlo de otra forma, las características del contacto en Internet restringen a algunos bienes y algunos comportamientos en los que la fisicidad no es un rasgo esencial, los objetivos realmente adecuados para un ciberataque y así, limitan el potencial incremento de los delitos en el ciberespacio.

Y junto a lo anterior, debe añadirse como factor relevante, el propio hecho de que, pese a la popularización del ciberespacio, tal ámbito aún no esté al alcance de muchas personas, de un sector de la población que apenas entra y usa Internet y, por tanto, no puede cometer delitos en el mismo. Incluso podríamos, aunque ello merecería de un estudio mucho más complejo, relacionar la criminalidad en el ciberespacio y la criminalidad en el espacio físico, con los caracteres sociales o psicológicos de las personas que acceden o no a Internet. Es indudable que hay un sector de la ciudadanía que delinque en el espacio físico y no puede hacerlo en el ciberespacio al no acceder a él[113].

Todo esto puede servir para contrarrestar parcialmente lo que anticipa la aplicación abstracta de los presupuestos de la TAC al ciberespacio: un aumento del crimen en el ciberespacio conforme los comportamientos en sociedad vayan realizándose también en este nuevo ámbito de intercomunicación personal que acerca a personas sin restricción de distancias.

No puede negarse, sin embargo, que estas expectativas de crecimiento de la cibercriminalidad, parecen chocar violentamente con el escasísimo impacto del ciberdelito en los tribunales de justicia. En Inglaterra, Wall recuerda que en 15 años de la Computer Misuse Act de 1990, tan sólo ha habido alrededor de los 200 enjuiciamientos[114]. En España, las Memorias anuales de la Fiscalía General del Esta-

control de los genes o los alimentos se lleve, como así sucede en muchos casos, por medio de sistemas electrónicos que podrían ser alterados por parte de un *hacker* desde otro lugar del mundo.

[113] Supondría, a mi parecer, sin embargo, un error de planteamiento, el pensar que hay algún tipo de condicionante psicológico, de carácter cognitivo o conductual-aprendido, relacionado con la criminalidad en el espacio físico que no se da en el ciberespacio. Más bien, lo que ocurrirá, es que los condicionantes del actuar criminal que generalmente se estudian en relación con delitos violentos, tales como la impulsividad, la agresividad, etc., aquí no serán tan determinantes por el tipo de crimen cometido. Pero esto no significa que el ciberespacio no pueda ser un ámbito para el delito, ni que las características generales de quienes acceden a él les hagan menos propensos al comportamiento criminal. Por el contrario, algunos estudios demuestran que los mismos elementos que influyentes teorías criminológicas, como la del autocontrol, han encontrado esenciales para el actuar delictivo, lo pueden ser también para los delitos cometidos en el ciberespacio, como los de piratería intelectual. Así, el estudio de HIGGINS, G. E./FELL, B. D./WILSON, A. L.: "Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States", en *SSCR,* núm. 25, 2007.

[114] WALL, D. S.: "Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime", en *International Review of Law Computers & Technology,* vol. 22, núm. 1–2, March–July, 2008,*ob. cit.,* p. 45.

do[115] constatan que si bien esta delincuencia va a más, los expedientes existentes aún son poco significativos en comparación con lo que, en otros estudios, parece reflejarse. De hecho, las fiscalías están incluso recurriendo a las Fuerzas y Cuerpos de Seguridad del Estado para obtener información fidedigna acerca del número de delitos perseguidos. Por citar un ejemplo, en un informe del Fiscal de delitos informáticos de la Audiencia Provincial de Málaga se certificó que la Policía Nacional y la Guardia Civil habían iniciado 294 atestados por delitos de tipo informático, de los que la Policía pudo esclarecer únicamente el 66%.

La cuestión, por tanto, y como ha señalado Wall, es si la escasez de procesos judiciales por cibercrímenes se debe a la ausencia de pruebas para la imputación de los mismos o más bien a la propia ausencia de cibercrímenes[116], esto es, si en realidad hay una sobredimensión de la amenaza del cibercrimen o una pobre respuesta judicial al mismo debido a factores varios todos más o menos directamente relacionados con la novedad del fenómeno y el anquilosamiento espacial-territorial del sistema de administración de justicia.

Pues bien, no puede negarse, como ha señalado acertadamente Guinchard, que el discurso sobre las amenazas cibernéticas tiende a estar dominado por el exceso de publicidad dada a algunas amenazas en perjuicio de los demás, y por las afirmaciones exageradas sobre la frecuencia y magnitud de los ataques[117]. Sin embargo, ello no es incompatible con la afirmación, también admitida por Guinchard y por toda la doctrina que se ha ocupado del cibercrimen[118], de que existe una importante cifra negra en materia de cibercriminalidad, esto es, que los delitos que se cometen son muchos más que los que aparecen en las estadísticas oficiales al ser enjuiciados y condenados como tales, hasta el punto de que hay quien ha señalado que la cibercriminalidad es la forma de delincuencia más infra-denunciada de toda la existente[119].

Lo cierto es que hay datos, y no meras hipótesis, que certificarían que con la ci-

[115] Véanse las Memorias de la Fiscalía General del Estado 2009 y 2010.

[116] WALL, D. S.: "Cybercrime, media and…",*ob. cit.,* p. 46.

[117] GUINCHARD, A.: "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy", en *Journal of Strategic Security,* vol. 4, núm. 2, 2011, p. 86. Véase sobre el miedo al cibercrimen el estudio de DE LA CUESTA ARZAMENDI, J. L. Y SAN JUAN GUILLÉN, C.: "La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad", en DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.): *Derecho penal informático,* Civitas, Cizur Menor, 2010. pág. 66 y ss.

[118] GONZÁLEZ RUS, J.J.: "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *Revista de la Facultad de Derecho de la Universidad Complutense de Madrid,* núm. 12, 1986, p. 109; ROVIRA DEL CANTO, E.: *Delincuencia informática y fraudes informáticos,* Comares, Granada, 2002, p. 90; DE LA CUESTA ARZAMENDI, J. L./PÉREZ MACHÍO, A. I.: "Ciberdelincuentes y cibervíctimas", en DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.): *Derecho penal informático,* Civitas, Cizur Menor, 2010.pág. 116 y ss; SIMION, R.: "Cybercrime and its challenges between reality and fiction. Where do we actually stand?", en *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. 3, núm.3- vol. 4, núm. 1, Settembre 2009-Aprile 2010, p. 306; HERRERA MORENO, M.: "El fraude informático en el Derecho penal español", en *Actualidad Penal,* núm. 39, La Ley, Madrid, 2001, p. 932; MORÓN LERMA, E.: *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red,* Aranzadi, Cizur Menor, 2ª edición, 2002, p. 37; y REINA ALFARO, L. M.: La víctima en el delito informático, p. 8, en Internet en http://www.ieid.org/congreso/ponencias/Reina%20Alfaro,%20Luis%20M.pdf. Citado el 28 de agosto de 2011.

[119] KSHETRI, N.: "The Simple Economics…", *ob. cit.*

bercriminalidad ocurriría algo similar a lo que sucede con los icebergs, que lo que se percibe o visualiza, es tan sólo un porcentaje ínfimo en comparación con lo que realmente existe[120]. Variados estudios insisten en que el cibercrimen está en crecimiento desde hace más de 10 años, siendo múltiples los ataques recibidos diariamente en nuestro país, algunos de los cuales no son propiamente delictivos (el caso del envío de*spam*) pero otros sí, como los daños, el acceso informático ilícito, las injurias y las calumnias, los ataques de DoS, etc. Así lo ponen de manifiesto numerosos informes independientes de algunas importantes empresas de seguridad como Javelin[121], que en su estudio sobre fraude de identidad, detectó un incremento de un 12% de víctimas de esta modalidad de ciberdelito, o el informe encargado a Pricewaterhouse Coopers[122], en el que pone de manifiesto que, mientras que en un estudio de 2008 sobre brechas de seguridad en las empresas, el 21% de los encuestados declararon haber sido infectados por virus u otro software malicioso, en 2010 esta cifra ascendió al 61%. Este mismo informe destaca otro dato llamativo: únicamente el 16% de las empresas encuestadas esperan un número menor de ataques en el año próximo. Otros informes publicados por instituciones gubernamentales o auspiciadas por los gobiernos, como el Internet Crime Complaint Center (IC3)[123], constatan que las denuncias por cibercrímenes pasaron de 16.838 en 2000 a 303.809 en 2010[124]. También parecen certificar esta tendencia de incremento del cibercrimen, otro tipo de estudios contra los que no podrá argumentarse, como se hace con los realizados por empresas de software, la falta de imparcialidad. Me refiero a las investigaciones sobre victimización en el ciberespacio que abarcan muchos tipos de ciberdelitos, si bien se ocupan más especialmente de las infecciones de *malware,* el *phishing,* el *cyberbullying,* el *online grooming* o el *cyberstalking.* Todas las investigaciones que he citado en este trabajo reflejan un aumento de la criminalidad, si bien debe reprocharse a las mismas que ninguna de ellas cuestiona las razones por la falta de denuncia de estos delitos.

Por último, y como argumentos a favor de la existencia de mayor cibercriminalidad, también debieran tomarse en cuenta las obvias razones para la falta de denuncia de la víctima del cibercrimen (el que el mismo pasa generalmente directamente inadvertido[125]; el que en muchos casos se percibe cuando ya no es posible o eficaz la denuncia[126]; el que la propia víctima ni siquiera valora el ciberataque como

[120] FAFINSKI, S; MINASSIAN, N.:*UK Cybercrime Report 2009*, Invenio Research, September, 2009, p. 23.

[121] En Internet en https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail. Citado el 29 de agosto de 2011.

[122] En Internet en http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf. Citado el 29 de agosto de 2011.

[123] El IC3 es una iniciativa fruto de la colaboración entre el FBI, el centro nacional para la criminalidad de cuello blanco (NW3C) y la oficina de asistencia a la justicia (BJA).

[124] GUINCHARD, A.: "Between Hype…",*ob. cit.,* p. 80.

[125] FAFINSKI, S; MINASSIAN, N.:*UK Cybercrime..., ob. cit.,* p. 23.

[126] ADLER, F./MUELLER, G. O. W./LAUFER, W. S.:*Criminology and the Criminal..., ob. cit,*.p. 351. DE LA MATA BARRANCO, N. J./PÉREZ MACHÍO, A. I.: "La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española", en DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J.

conducta delictiva[127], el que se suele infravalorar su importancia[128], la falta de confianza en las autoridades judiciales para la averiguación de los hechos[129], la publicidad negativa que conllevaría para las empresas el reconocimiento del ataque sufrido[130], etc.), así como la evidencia de las mayores complicaciones generales de los procesos judiciales contra gran parte de los cibercrímenes que los que se inician contra crímenes en el espacio físico[131].

Todo ello parece ponerse del lado de quienes creemos que el delito en el ciberespacio es mayor de lo que dicen las estadísticas. También apoyaría la tesis aquí defendida, a partir de la abstracción de la TAC en el nuevo ámbito de oportunidad que es el ciberespacio, de que el delito aumentará en Internet especialmente mientras no se perciban sus peculiaridades y no se refuercen los mecanismos de protección que la propia víctima puede imponer frente al cibercrimen. En todo caso, entre la aceptación como verdad única de unos datos oficiales lastrados por la complejidad de la adaptación del sistema penal a un nuevo ámbito como es el ciberespacio, o la afirmación como realidad de algo no contrastado, tenemos que seguir quedándonos con la investigación seria y rigurosa del fenómeno, con su intento de comprensión para tratar de dimensionar lo más precisamente, y si es posible con estudios empíricos, el mismo, por lo que es necesario seguir pensando sobre cómo es y porqué el delito en el ciberespacio así como tratar de contrastarlo pese a la dificultad que aún ello conlleva.

(COORD.): *Derecho penal informático, ob. cit.,* p. 116; y ROMEO CASABONA, C.M.: *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información,* Fundesco, Madrid, 1988, p. 38.

[127] FAFINSKI, S; MINASSIAN, N.:*UK Cybercrime…, ob. cit.,* p. 23.

[128] Como señala GUINCHARD, sin embargo, los criminales cibernéticos aprovechan esa subestimación crónica de los delitos cibernéticos, puesto que una pérdida de 30 libras o euros para una persona puede significar una ganancia mínima de 3.000 al infractor, ya que las estafas se dirigen a cientos de miles de personas en línea GUINCHARD, A.: "BetweenHype...", *ob. cit.,* p. 80.

[129] KSHETRI, N.: "The Simple Economics…",*ob. cit.*

[130] GALÁN MUÑOZ, A.: Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en Revista de Derecho y Proceso Penal, ISSN 1575-4022, Nº. 15, 2006, pp. 18 y 19.

[131] La razón principal es que cuando existe una denuncia, generalmente en estos casos no dirigida contra alguien en concreto sino reflejando una concreta victimización (un dinero defraudado por un usuario indeterminado, un daño en el sistema por un virus, una calumnia en una página web, etc.), los primeros pasos de la investigación policial se dirigen hacia la determinación de los autores, y hay varios motivos por los que ésta puede ser especialmente complicada para estos delitos. En primer lugar, por las propias características, favorecedoras del anonimato, del ciberespacio: aunque el ciberdelito es cometido por alguien en concreto, en Internet sólo se muestra una representación virtual del autor (la dirección IP), que puede ser concretada, pero a la que después hay que atribuir la concreta persona física que está detrás de la acción, y eso ya es más complicado, pues exige, primero, la colaboración de las empresas proveedoras de servicios y, después, la investigación del titular del sistema informático desde el que se ha realizado el ataque y la concreción, de entre todos los usuarios del mismo, del que en particular lo ha ejecutado[131]. En segundo lugar, y relacionado con lo primero, la determinación judicial de las personas autoras del cibercrimen suele complicarse debido a la transnacionalidad del delito. Ya no se trata, como en la criminalidad física, de que el delincuente haya podido trasladarse a otro país tras cometer el delito y haya que solicitar su entrega a las autoridades judiciales españolas, sino de que el delito haya sido directamente cometido desde el extranjero, con lo que los procesos para la identificación del cibercriminal requieren de la, no siempre sencilla tarea de lograr, colaboración de otros Estados. Al fin y al cabo, no es lo mismo solicitar la extradición de una persona concreta por la comisión de un determinado delito, que solicitar a un Estado extranjero que investigue quién puede ser el sujeto que se halle detrás de una concreta IP que presuntamente puede haber perpetrado una infracción penal. La práctica judicial demuestra que la Fiscalía suele cesar en el intento de identificación cuando la IP se encuentra en Rusia o países similares relacionados con mafias de cibercriminales.

3.2. *Old wine in different bottles*: particularmente, el protagonismo de la víctima en el cibercrimen y su prevención

Decíamos anteriormente que el cibercrimen seguía siendo un delito, pero que los caracteres intrínsecos y extrínsecos definitorios del nuevo ámbito en el que se realiza el mismo, nos obligaban a replantear las teorías que tratan de explicar el delito, así como de prevenirlo al nuevo ámbito de riesgo que es el ciberespacio. Trató de expresar esto, probablemente, Grabosky, cuando señaló que el cibercrimen era: el vino de siempre en botellas diferentes. El sentido acertado, de los tres posibles que señalábamos anteriormente, no es el de que el crimen (como evento) sólo cambia en apariencia al realizarse en Internet; tampoco es el de que el cibercrimen no es ya siquiera un crimen; por el contrario el cibercrimen, como evento social, sigue estando conformado por los mismos elementos que, sin embargo, al producirse en un ámbito tan distinto como es el ciberespacio, confluyen de distinta forma a como lo hacían en el espacio físico. En realidad, por tanto, creo que sería mejor afirmar que el cibercrimen es el mismo vino pero en botellas distintas, no ya sólo nuevas, sino diferentes, en las que probablemente la forma tradicional de beber ya no sea válida. Al final, siguiendo con el símil brevemente, se tratará de beber vino, pero tenemos que replantearnos cómo hacerlo, dado que el recipiente desde el que se ingiere es ahora otro.

El primer paso, por tanto, es lo que, modestamente, he tratado de hacer en este artículo: comprender mejor el nuevo ámbito de oportunidad criminal y definir los elementos del delito y su confluencia en él. La contracción de la distancia en Internet y la consiguiente expansión comunicativa unidas a la popularización del ciberespacio transnacional, anónimo y sujeto a revolución permanente, conlleva que los eventos criminales en él sean distintos, incidiendo tales caracteres en un agresor motivado que tiene menos barreras temporales y espaciales para el delito, que tiene menos control sobre los efectos del crimen, etc; en unos gestores con un ámbito de incidencia muy limitado para las amplias dimensiones del ciberespacio; y en unas víctimas u objetivos adecuados que con su comportamiento definen significativamente el ámbito de riesgo al que están sometidos. Porque si bien son múltiples y variados, y todos ellos deben ser analizados en profundidad, los cambios que el ciberespacio supone como ámbito de oportunidad criminal, y si se ven modificados significativamente todos los elementos del delito, destaca de forma obvia por encima de todos el importante papel condicionante de la víctima en el cibercrimen[132], a mi parecer de forma aún más pronunciada que en el delito en el espacio físico.

En efecto, si bien hemos insistido en que lo relevante en el delito como evento no es cada uno de los elementos del mismo como su confluencia, ésta, cuando se

[132] También en este sentido, DE LA CUESTA ARZAMENDI, J. ./PÉREZ MACHÍO, A. I.: "Ciberdelincuentes y cibervíctimas", en DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.): *Derecho penal informático,* Civitas, Cizur Menor, 2010.pág. 115.

produce en el ciberespacio, parece reflejar un mayor protagonismo, no frente a los otros elementos pero sí frente a lo que tiene generalmente en el espacio físico, del objetivo o víctima del delito. 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 (the random fallacy)[133]. 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[134]. Lo hace, sin duda, al actuar con una voluntad criminal, pero lo hará únicamente sobre aquél 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.

En efecto son, a mi parecer, tres los factores que hacen que la víctima adquiera una especial importancia para la explicación y prevención del delito en el ciberespacio. El primero, y 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. Pero seguirían pudiendo robarle (matarle o violarle) yendo a su domicilio, lo cual no es posible en Internet si la víctima no introduce en él los bienes de que se trate. Al fin y al cabo en el ciberespacio no está la persona sino una expresión suya por ella misma elegida.

En segundo lugar la víctima define con su interacción en el ciberespacio el grado

[133] FELSON, M./BOBA, R.:*Crime and everyday…, ob. cit.,* p. 21

[134] Obviamente tampoco lo era antes de forma absoluta, pero intuitivamente, y como posteriormente se explicará, parece que la víctima es ahora más protagonista que en el espacio físico.

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 cibercriminalidad informática. Así, Alshalan[135] logra relacionar la victimización con la interacción de la víctima en el ciberespacio, y en el mismo sentido se sitúan los analizados estudios de Yucedal y Choi. 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 el que la misma afecte a uno, dos, cientos o miles de personas dependerá mucho de lo que hagan estas. También cambia que mientras que ya hemos identificado en el espacio físico, y para determinado tipo de delitos, las conductas que pueden resultar peligrosas, aún no nos hemos preguntado todavía sobre cuáles son los comportamientos de riesgo en Internet, y es indudable que resultará esencial hacerlo de cara a la prevención de este tipo de criminalidad.

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 éste 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, también al no existir distancias, el desplazamiento del cibercriminal hacia otros objetivos resulta, no sólo 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 ésta, de victimización. Claro que la víctima también influye en la capacidad de sus guardianes en el espacio físico, pero si bien no se venden casas sin puertas o cisos en urbanización sin vecinos, sí se venden sistemas informáticos con acceso a redes sin antivirus o sin actualización de los mismos así como redes sociales y demás lugares de comunicación social sin información sobre los riesgos de su uso.

Evidentemente, no son los condicionantes derivados de la TAC los únicos que

[135] ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* p. 123.

inciden en la cibervictimización. Los estudios analizados ponen de manifiesto que hay factores demográficos también relevantes a la hora de la mayor o menor victimización: en los realizados en EEUU se confirma que las personas de raza blanca tienen un mayor riesgo de victimización, y lo mismo ocurre en general con los varones frente a las mujeres,[136] lo cual, por otra parte, y de nuevo acercándonos a la TAC, se corresponde con la frecuencia de uso de Internet y la duración del tiempo pasado en el ciberespacio, que son mayores en los varones, como se muestra en la tabla basada en el estudio deAlshalan[137]. Es cierto, sin embargo, que la diferencia entre el tiempo de uso de Internet entre hombres y mujeres no es estadísticamente significativa, por lo que quizás debiera tenerse en cuenta el tipo de actividad cotidiana *on line* que realizan los hombres (especialmente en cuanto a descarga de archivos o actividad de comercio electrónico), frente al que realizan las mujeres, para entender el mayor riesgo de victimización del hombre[138]. También está generalmente admitido que el tiempo de uso en Internet es significativamente mayor en los usuarios jóvenes frente a los más mayores. Concretamente en el estudio de Pratt *et al.* sobre victimización por ciberfraude, se señala que, por cada unidad en la que se incrementa la edad, disminuye en tres unidades porcentuales el tiempo pasado en el ciberespacio durante la semana[139]. Puede decirse, por tanto, que hay un mayor riesgo de victimización en el ciberespacio para los jóvenes, si bien de nuevo ello pueda estar derivado del estilo de vida de los mismos, concretamente de las horas que suelen pasar en Internet.

Y es que el análisis comparado de los estudios revisados nos lleva a la conclusión, como también a los autores que los han desarrollado, que los factores demográficos son menos relevantes que las actividades cotidianas en Internet llevadas a cabo por las víctimas. Así lo demuestran los estudios empíricos conforme a los cuales, cuando se incluyen las variables derivadas de la teoría de las actividades cotidianas, los efectos de la edad, la educación y otros sobre la victimización por cibercrímenes, son eliminadas[140].

Todo lo anterior se resumiría, por tanto, en la afirmación de que la falacia del crimen azaroso que constata Felson y conforme a la cual la gente cree, erróneamente, que el delito sucede independientemente de lo que ella haga y como ella actúe, como una desgracia ajena a su comportamiento, lo es aún más, o quizás se mani-

[136] ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* p. 146.

[137] ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* p. 83.

[138] También puede ser relevante el factor medio al delito, que es mayor en mujeres que en hombres, conforme al propio estudio de ALSHALAN (ALSHALAN, A.: *Cyber-CrimeFear..., ob. cit.,* pp. 145 y ss.), aunque son menos susceptibles de ser victimizadas. Sería interesante analizar en qué medida el miedo al delito, condiciona las concretas actividades realizadas por las mujeres frente a los hombres en el ciberespacio.

[139] PRATT, T.C./HOLTFRETER, K./REISIG, M. D.: "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory", en *Journal of Research in Crime and Delinquency,* vol. 47, núm. 3,2010.

[140] ALSHALAN, A.: *Cyber-Crime Fear..., ob. cit.,* p. 146. En el mismo sentido, PRATT, T.C./HOLTFRETER, K./REISIG, M. D.: "Routine Online…", *ob. cit.,* p. 267.

fiesta de forma más expresiva, en el ciberespacio[141]. Qué duda cabe de que lo afirmado tiene importantes consecuencias prácticas a efectos preventivos: 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. Sobre ello, en todo caso, habría mucho más que decir.

3.3. **Líneas de futuro: de las actividades cotidianas a la prevención (situacional) del cibercrimen.**

Dice Pease que la teoría de la prevención de la delincuencia se ocupa de comprender los mecanismos que causan el evento criminal, siendo la cuestión central el cómo lograr perturbarlos[142]. A mi parecer, es esencial comprender en primer lugar, que el cibercrimen como evento, tiene mucho que ver con las decisiones que adopta la víctima en su día a día, con sus actividades cotidianas y con la (escasa) percepción del riesgo de las mismas, y la cuestión central debe ser, por tanto, la de mejorar su protección como forma de, en términos de prevención situacional, aumentar el esfuerzo necesario para la realización del delito.

Admitida pues, como conclusión, la extraordinaria relevancia de la conducta de la víctima en relación con la cibercriminalidad, su corolario es la necesidad de perturbar las facilidades que la víctima suele poner para el delito en el ciberespacio, en aras de reducir este tipo de delincuencia. La prevención de la cibercriminalidad, pues, requerirá la adopción de medidas que permitan a la víctima convertirse en su propio guardián capaz y, a la vez, evitar la realización de las conductas que facilitan la ejecución del delito. Aumentar su formación para una mejor autoprotección y para la adopción de rutinas seguras, potenciar la utilización de sistemas de autoprotección que eviten riesgos no deseados, e incluso enseñar a limitar los bienes personales y patrimoniales que pone en contacto con el ciberespacio, deberían ser objetivos político-preventivos básicos en relación con la cibercriminalidad.

Obviamente, la víctima no es un elemento que pueda tomarse en cuenta de forma separada y única para la prevención del cibercrimen. La prevención del cibercrimen deberá atender esencialmente, paralelamente a la intervención social y jurídica que trate de motivar al sujeto a la no realización de conductas criminales, a tratar de perturbar la decisión del cibercriminal de serlo, incrementando lo que percibe que le puede costar lograr su objetivo, aumentando el riesgo percibido de que al hacerlo

[141] FELSON, M./BOBA, R.:*Crime and everyday…, ob. cit.,* p. 21.

[142] PEASE, K.: "Crime Prevention", enMAGUIRE, M./MORGAN R./REINER, R.:*The Oxford handbook*…, *ob. cit.,* pp. 963 y ss.

sea capturado (en términos judiciales), y reduciendo los beneficios que valore que podrá obtener de su actividad[143], logrando así que no lleve a cabo la conducta.

Entramos aquí de lleno, pues, en el enfoque de la prevención situacional, partiendo como presupuesto de la teoría de la elección racional, esto es, de la idea de que la conducta delictiva deriva de un proceso racional de toma de decisiones en el que el sujeto actúa con una determinada finalidad eligiendo entre las opciones que tiene[144]. Puede parecer extraño el referirse a la prevención situacional del crimen en el ciberespacio, sobre todo si se identifica este enfoque únicamente con la modificación del ambiente físico, del espacio geográfico en el que se produce el evento criminal. No lo es tanto, si lo interpretamos como lo que es: un modelo de prevención del delito que, frente a las tradicionales teorías de la criminalidad que se interesan por las razones que llevan a las personas a convertirse en delincuentes, pone el énfasis en la importancia de los factores ambientales, es decir, en la existencia de lugares y momentos que propician la concentración de los delitos, lo que permite la intervención en el ámbito de oportunidad para reducirla y evitar que el criminal motivado pueda cometer el delito. Es obvio que el ciberespacio es también ambiente, concretamente es un nuevo ámbito de oportunidad criminal y por eso es adecuado acercarse al crimen que se desarrolla en dicho nuevo espacio desde el enfoque que parte de la premisa de que las características del lugar donde se produce el delito condicionan el mismo y por ello, de que puede intervenirse en ellas para prevenir su realización.

Aplicado a lo que nos interesa, a la cibercriminalidad y su prevención, de lo que se trataría es de aprovechar las enseñanzas anteriores sobre la modificación del ámbito de oportunidad criminal en el ciberespacio, para tomar medidas en materia de educación de la víctima, en su actuar cotidiano y en la incorporación de autoguardianes capaces, que influyan en la decisión del cibercriminal, especialmente en lo relativo a la valoración del esfuerzo que va a tener que realizar para cometer el delito. La utilización de medidas de protección tecnológica por parte de la víctima o la existencia de sistemas de vigilancia y demás, serán tomados en consideración por parte del agresor potencial, desincentivando una primera decisión de cometer el ataque en el ciberespacio. Por el contrario, la inexistencia de estas medidas de tutela convierte a la víctima en objetivo adecuado contra el que es sencillo perpetrar el ataque y en objeto de preferencia por parte del cibercriminal. También es importante desde esta perspectiva, la percepción de la ganancia que se obtendrá fruto de la actividad criminal, lo cual parte de la idea anteriormente comentada, relativa a que el delito tiene un carácter instrumental, en el sentido de que responde a la voluntad de consecución de objetivos básicos de los delincuentes, tales como dine-

[143] Clarke, R.V.: "Introduction." In: Clarke, R. V (ed.).:*Situational Crime Prevention: Successjul Case Studies.* Albany (NY), 1992.

[144] Sobre la idea del crimen como comportamiento instrumental orientado a la consecución de necesidades básicas del delincuente, véase, CORNISH, D.B./CLARKE, R. V.: *The reasoning Criminal…, ob. cit.*

ro, sexo, estatus y aventura[145]. Como se ha visto al explicar el ámbito de oportunidad criminal que es el ciberespacio, existe en él un aumento potencial significativo de las posibilidades de contacto entre agresor motivado y víctima debido a la destrucción de la distancia física como obstáculo para la comunicación directa entre personas y el acceso a los bienes. Precisamente por ello, medidas tendentes a la ocultación de objetivos y demás formas de minimización de las posibles ganancias o recompensas que el agresor percibirá que puede obtener, podrían tener gran éxito.

Y también tienen que ver con la motivación del agresor para la comisión del cibercrimen, otros dos conjuntos de técnicas de prevención situacional, las medidas relativas al incremento del riesgo percibido y las tendentes a incrementar la vergüenza o culpabilidad del delincuente. Es indudable que el ciberespacio es un ámbito que, además de que permite que se oculte la existencia de delito o de sus efectos durante mucho tiempo, favorece el anonimato de quien lleva a cabo la infracción criminal, pero no es imposible pensar en medidas para aumentar la percepción de inseguridad del cibercriminal, lo cual debería pasar por incrementar el número de guardianes, por facilitar la identificación de los usuarios y demás medidas.

En cuanto a la potenciación de los sentimientos de culpabilidad asociados a la realización del comportamiento criminal, tampoco es el ciberespacio un ámbito en el que vaya a ser esta tarea sencilla, especialmente en relación con algunas conductas criminales que, pese a serlo, están prácticamente aceptadas como adecuadas por parte de los usuarios que acceden regularmente a La Red. Pero precisamente por ello, debiéramos reflexionar acerca de la necesidad de incidir en la valoración social de las conductas y en la legitimidad de sus sanciones, porque sólo con las normas o con la amenaza de ser cazado, no se prevendrá el cibercrimen.

El de construir un sistema de prevención situacional del cibercrimen, será un camino largo y complicado que, obviamente, no puedo continuar presentando aquí dada la extensión del trabajo. Simplemente, he pretendido iniciar su exposición creando unas bases que deberán reforzarse posteriormente con una mayor profundización teórica y, desde luego, con la realización de estudios empíricos que traten de, por una parte, certificar la validez de las teorías que aquí he enunciado ypor otra, de constatar la eficacia de las medidas de prevención situacional que vayamos proponiendo. Será necesario además, tener en cuenta las numerosas e importantes críticas al enfoque de la oportunidad en general, y a la teoría de la prevención situacional en particular[146], y valorarlas tanto en lo ético como en lo práctico.

[145] Recuerda MEDINA ARIZA ésta como una de las argumentaciones básicas del enfoque de la prevención situacional. MEDINA ARIZA, J. J.: "El control social…", *ob. cit.*, p. 286.

[146] Si bien no procede aquí ni una completa revisión de todas las críticas a las teorías de la oportunidad y al enfoque de la prevención situacional, ni su valoración, sí que debe destacarse que su utilización no es pacíficamente aceptada, especialmente por la teoría criminológica más tradicional y por la nueva criminología sociológica que, especialmente, intuye problemas éticos y de legitimidad de su utilización que fueron puestos de manifiesto y recopilados en el libro colectivo VON HIRSCH, A./GARLAND, D./WAKEFIELD, A.: *Ethical and Social Perspectives on Situational Crime Preven-*

En todo caso, comenzar a transitar el mismo, no implica afirmar que es éste el enfoque único desde el que deben centralizarse las políticas de prevención del crimen en el ciberespacio. La utilización aquí de esta perspectiva criminológica para la recomendación de medidas preventivas frente a la cibercriminalidad, ni supone dejar de lado cualesquiera otras perspectivas más centradas en lo estructural, ni tampoco la consideración de que este enfoque es el central que debe tomarse en materia de prevención del delito. Simplemente, conlleva la afirmación de que si el delito se produce en un espacio, el que se ejecuta en el ciberespacio debe ser distinto, y comprender el alcance de esta afirmación debe ser el primer paso para poder prevenirlo de forma eficaz.

BIBLIOGRAFÍA

Adler, F./Mueller, G. O. W./Laufer, W. S.: *Criminology and the Criminal Justice System*, McGraw Hill, New York, 2001 (4ª edición).

Aguirre Romero, J. Mª: "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI", en *EREL*, Universidad Complutense de Madrid, núm. 27, julio/octubre, 2004, en Internet en http://www.ucm.es/info/especulo/numero27/cibercom.html. Citado el 1 de octubre de 2010.

Agustina Sanllehí, J.R.: "La arquitectura digital de Internet como factor criminógeno", en *IECS,* art. 4, núm. 3, 2009.

Alcantara, J.: *La neutralidad en La Red, y porqué es una mala idea acabar con ella*, Biblioteca de Las Indias, Bilbao-Madrid-Montevideo, 2011.

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

Beebe, N. L./Rao, S. V: "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security", en *Proceedings of the 2005 SoftWars Conference,* Las Vegas, NV, Dec 2005.

tion, Hart Publishing, Oxford-Porltand, 2000, y en otros trabajos posteriores, como en GARLAND, D.: *The Culture of Control…, ob. cit.* pp. 130 y ss., donde, siguiendo con la línea argumentativa de sus dos artículos en el citado libro, GARLAND, D.: "Ideas, Institutions and Situational Crime Prevention", y GARLAND, D.: "The new criminologies of Everydaylife: Routine Activity Theory in Historical and social context", ambos en VON HIRSCH, A./GARLAND, D./WAKEFIELD, A.: *Ethical and Social…, ob. cit.,* pp. 1 y ss., y 215 y ss.,señala que, frente al tratamiento del crimen por la criminología tradicional como un problema con dimensiones sociales, temporales y psicológicas, el modelo de la decisión racional lo hace como una cuestión de precio, lo cual puede conllevar una legitimación de políticas duras en los que la eficacia de la intervención se sobrepone a otros valores. En nuestro país, estas cuestiones las analizó primero MEDINA ARIZA, J. J.: "El control social…", *ob. cit.,* p. 286, y lo ha hecho más recientemente, en un libro colectivo. Sin entrar en una, imposible aquí, evaluación de las críticas y sus argumentos, lo cierto es que el riesgo del enfoque situacional y, en general, de las teorías de la oportunidad, estriba en no prestar atención, desde una perspectiva global y para la prevención del crimen, a los aspectos sociológicos y psicológicos del delito, al igual que algunas teorías criminológicas se centran demasiado en lo explicativo y no aportan auténticas soluciones para la prevención del crimen en contextos determinados. También es evidente que la aplicación de mecanismos de prevención situacional sin sometimiento a los principios y límites de la intervención penal y de la aplicación de políticas públicas de un Estado Social y Democrático de Derecho, resulta inaceptable, como lo es la aplicación de medidas de intervención social y psicológica a partir de los presupuestos de cualquiera de las teorías criminológicas tradicionales sin el respeto a los citados principios. Pero nada de ello deslegitima el enfoque de la prevención del crimen en el día a día, sino que, más bien, las sitúa como parte del análisis que debe realizarse para la prevención de la delincuencia y siempre en el marco de los límites que marca el Estado Democrático en el que vivimos.

Bottoms, A. E/ Wiles, P.: "Environmental Criminology", en Maguire, M./Morgan R./Reiner, R.: *The Oxford handbook of criminology,* Oxford University Press, 2ª ed, New york, 1997.

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

Brenner, S. W.: "Cybercrime Metrics. Old Wine, New Bottles?", en *VJOLT***,** vol. 9, núm. 13, 2004.

Brenner, S. W y Clarke, L. L.: "Distributed Security: preventing cybercrime", en *TJMJCIL,* Summer 2005.

Capeller, W.: *"*Not such a neat net: some comments on virtual criminality", en *SLS,* núm. 10, 2001.

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

Cialdini, R.B./Kallgeren, C.A./Reno, R.R.: "A focus theory of normative conduct: When norms affect and do not affect behavior", en *PSPB,* vol. 26, núm. 8, 2000.

Cialdini, R.B./Kallgeren, C.A./Reno, R.R: "A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior", en *AESP,* núm. 24, 1991.

Clarke, R.V.: "Introduction." In: Clarke, R. V (ed.).:*Situational Crime Prevention: Succesjul Case Studies.* Albany (NY), 1992.

Clarke, R. V.: "Hot products: understanding, anticipating and reducing demand for stolen goods", en *Paper nº 112, Police Research Series,* British home Office Research Publications, London, 1999.

Clarke, R. V./Felson, M.: "Introduction: Criminology, routine activity, and rational choice", en Clarke, R./Felson, M.(Eds.): "Routine activity and rational choice", en *ACT,* vol. 5, Transaction Publishers, New Brunswick, New Jersey, 1993.

Clough, J.: *Principles of Cybercrime,* Cambridge University Press, Cambridge, 2010.

Cohen, L./Felson, M.: "Social change and crime rate trends: A routine activity approach", en *ASR,* vol. 44, núm. 4, 1979.

Davidson, D.: *Essays on actions and events,* Clarendon Press, Oxford, 1980.

Davies, R./Pease, K.: "Crime, technology and the future", en *SJ*, núm. 13, abril, 2000.

De Andrés Blasco, J.: "¿Qué es Internet", en García Mexía, P. (Dir.): *Principios de Derecho de Internet,* Tirant lo Blanch, Valencia, 2002.

De la Cuesta Arzamendi, J. L. (Dir.)/De la Mata Barranco, N. J. (Coord.): *Derecho penal informático,* Civitas, Cizur Menor, 2010.

De la Cuesta Arzamendi, J. L./Pérez Machío, A. I.: "Ciberdelincuentes y cibervíctimas", en De la Cuesta Arzamendi, J. L. (Dir.)/De la Mata Barranco, N. J. (Coord.): *Derecho penal informático,* Civitas, Cizur Menor, 2010.

De La Cuesta Arzamendi, J. L. y San Juan Guillén, C.: "La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad", en De la Cuesta Arzamendi, J. L. (Dir.)/De **la** Mata Barranco, N. J. (Coord.): *Derecho penal informático,* Civitas, Cizur Menor, 2010.

De La Mata Barranco, N. J./Pérez Machío, A. I.: "La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española", en De la Cuesta Arzamendi, J. L. (Dir.)/De la Mata Barranco, N. J. (Coord.): *Derecho penal informático,* Civitas, Cizur Menor, 2010.

Fafinski, S; Minassian, N.: *UK Cybercrime Report 2009*, Invenio Research, September, 2009.

Farrell, G./Pease, K.: "Criminology and Security", en Gill, M (Ed.): *The Handbook of Security,* Perpetuity Press, 2005.

Felson, M,/Boba, R.: *Crime and everiday life,* Sage, Thousand Oaks, CA, 2009 (4ª edición).

Felson, M.: *Crime and everyday life,* Thousand Oaks, CA: Pine Forge Press, 1998 (2ª edición).

Felson, M.: "Technology, Business and Crime", en Felson M./Clarke, R.V. (ed.): *Business and Crime Prevention,* New York, 1997.

Felson, M.: "Linking criminal choices, routine activities, informal control and criminal outcomes", en Cornish, D.B./Clarke, R. V. (Eds.): *The reasoning Criminal, Rational choice perspectives on offending*, Springer-Verlag, New York, 1986.

Fuchs, C.: "Transnational Space and the "Network Society", en *Paper Presented at the Association of Internet Researchers (AoIR) Conference: Internet Research 7.0,* Brisbane, September 27-30, 2006, en Internet en http://aoir.org/files/fuchs_516.pdf, p. 9. Citado el 2 de diciembre de 2010.

Furnell, S.: "Cybercrime: vandalizing the information society", en *LNCS,* vol. 2722, 2003.

Galán Muñoz, A.: Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en Revista de Derecho y Proceso Penal, ISSN 1575-4022, Nº. 15, 2006, pp. 18 y 19.

Garland, D.: *The Culture of Control. Crime and Social order in contemporary society,* Oxford University Press, New York, 2001.

Garland, D.: "Ideas, Institutions and Situational Crime Prevention", en Von Hirsch, A./Garland, D./Wakefield, A.: *Ethical and Social Perspectives on Situational Crime Prevention,* Hart Publishing, Oxford-Porltand, 2000.

Garland, D.: "The new criminologies of Everyday life: Routine Activity Theory in Historical and social context", en Von Hirsch, A./Garland, D./Wakefield, A.: *Ethical and Social Perspectives on Situational Crime Prevention,* Hart Publishing, Oxford-Porltand, 2000.

Gibson, W.: *Neuromancer,* AceBooks, New York, 1984.

González Rus, J.J.: "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en RFDUCM*,* núm. 12, 1986.

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

Grabosky, P./Smith, R.: "Telecommunication fraud in the digital age: the convergence of technologies", en Wall, E. (Ed.): *Crime and the Internet*, London, Routledge, 2001.

Grabosky, P.: "Computer crime: a criminological overview", en *Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Treatment of Offenders,* Vienna, 15 de abril de 2000.

Graham, S.: "The end of geography or the explosion of place? Conceptualizing space, place and information technology", en *PHG,* vol. 22, núm. 2, 1998.

Green, N.: "On the Move: technology, mobility, and the mediation of social time and space", en *IS*, vol. 18, núm. 4, 2002.

Guinchard, A.: "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy", en *JSS,* vol. 4, núm. 2, 2011.

Gutiérrez Puebla, J.: "Redes, espacio y tiempo", en *AGUC,* núm. 18, 1998.

Herrera Moreno, M.: "El fraude informático en el Derecho penal español", en *Actualidad Penal,* núm. 39, La Ley, Madrid, 2001.

Higgins, G. E./Fell, B. D./Wilson, A. L.: "Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States", en *SSCR,* núm. 25, 2007.

Higgins G. E./Makin D. A.: "Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy?", en *IJCC,* primavera, vol. 2, 2004.

Hindelang, M. J./Gottfredson, M. R./Garofalo, J.: *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*, Cambrdige, MA, Balliger Publishing Company, 1978.

Holt, T. J./Bossler, A. M..:"Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization", en *DB*, vol. 30, núm. 1, enero, 2009.

Holt, T. J/Bossler, A. M.: "On-line Activities, Guardianship and Malware Infection: An Examination of Routine Activities Theory", en *IJCC,* vol. 3, núm. 1, enero-junio, 2009.

Hutchings, A./Hayes, H.: "Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?", en *CICJ*, vol. 20, núm. 3, marzo, 2009.

Jewkes, Y.: "Cybercrime", en Mclaughlin, E.U./Muncie, J. (Eds.).: *The Sage Dictionary of Criminology,* Sage, London -California, 2006.

Jones, B. R.: "Comment: virtual neighborhood watch: open source software and community", en *JCLC,* vol. 97, núm. 2, winter, 2007.

Kennedy, L.W./Gibbs van Bruschot, E.: "Routines and the criminal event", en Meier, R. F./ Kennedy, L. W./Sacco, V. F. (Eds.): *The Process and structure of Crime. Criminal events and Crime analysis,* en *ACT*, vol. 9, Transaction Publishers, New Jersey, 2001.

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

Kshetri, N.: "The Simple Economics of Cybercrimes", en *IEEE Security & Privacy,* The Ieee Computer Society, 2006, en Internet en http://see.xidian.edu.cn/ hujianwei/papers/098The%20Simple%20Economics%20of%20Cybercrimes.pdf

Lee, H./Liebenau, J.: "Time and the Internet at the turn of the millenium", en *TSoc.,* vol. 9, núm. 1, 2000.

Longe, O. B./Mbarika, V./Kourouma, M./Wada, F./Isabalija, R.: "Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities", en *IJCSIS,* vol. 6, núm. 3, 2009.

López Ortega, J. J.: "Libertad de expresión y responsabilidad por los contenidos en Internet", en *CDJ,* núm. 10, 2001.

Marcum, C. D.: "Adolescent online victimization and Constructs of Routine Activities theory", en Jaishankar, K (Ed.): *Cyber Criminology. Exploring Internet crimes and criminal behavior,* CRC Press, Boca Ratón, 2011.

Mayhew, P./Clarke, R./Sturman, A./Hough, M.: "Crime as opportunity", en *Home office Research Study,* núm. 34, London, 1976.

McQuade, S. C.: "Cybercrime", en Tonry, M (Ed.).: *The Oxford Handbook of Crime and public policy,* Oxford University Press, New York, 2009.

Medina Ariza, J. J.: "El control social del delito a través de la prevención situacional", en *RDPC*, 2ª época, nº2, 1998.

Meier, R. F./Kennedy, L. W./Sacco, V. F.: "Crime and the criminal event perspective", en Meier, R. F./ Kennedy, L. W./Sacco, V. F. (Eds.): *The Process and structure of Crime. Criminal events and Crime analysis,* en *ACT*, vol. 9, Transaction Publishers, New Jersey, 2001.

Mestre Delgado, E.: "Tiempos de cibercrimen", en *LL,* núm. 37, año IV, abril, 2007.

Morón Lerma, E.: *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red,* Aranzadi, Cizur Menor, 2002 (2ª edición).

Nisbett, C.: "New directions on Cybercrime", White Paper, Qinetiq, en Internet en http://apps.qinetiq.com/perspectives/pdf/EP_White_Paper3_Cyber%20Crime.pdf

Pease, K.: "*Science in the service of crime reduction"*, en Tilley, N. (Ed.): *Handbook of crime prevention and community safety,* Willan Publishing, UK, 2005.

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

Pérez Luño, A. E.: "Impactos sociales y jurídicos de Internet", en *ART,* núm. 1, 1998.

Pittaro, M. L.: "Cyber stalking: An Analysis of Online Harassment and Intimidation", en *IJCC*, vol. 1, núm. 2, 2007.

Pratt, T.C./Holtfreter, K./Reisig, M. D.: "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory", en *JRCD,* vol. 47, núm. 3, 2010.

Reina Alfaro, L. M.: La víctima en el delito informático, en Internet en http://www.ieid.org/congreso/ponencias/Reina%20Alfaro,%20Luis%20M.pdf. Citado el 28 de agosto de 2011.

Romeo Casabona, C. M.: "De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal", en Romeo Casabona, C.M. (Coord.): *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Comares, Granada, 2006.

Romeo Casabona, C.M.: *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información,* Fundesco, Madrid, 1988.

Rovira del Canto, E.: *Delincuencia informática y fraudes informáticos,* Comares, Granada, 2002.

Serrano Maíllo, *Introducción a la criminología*, Dykinson, Madrid, 2009 (6ª edición).

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

Simion, R.: "Cybercrime and its challenges between reality and fiction. Where do we actually stand?", en *RCVS*, vol. 3, núm.3- vol. 4, núm. 1, Settembre 2009-Aprile 2010.

Smith, R. G./Grabosky, P./Urbas, G.: *Cyber criminals on trial,* Cambridge University Press, Cambridge, 2004.

Svensson, J. S./Bannister, F.: "Pirates, sharks and moral crusaders: Social control in peer–to–peer networks", en *FMPRJI,* vol. 9, núm. 6 – 7, junio, 2004.

Thomas, D./Loader, B.: "Introduction – Cybercrime: Law enforcement, security and surveillance in the information age", en Thomas, D./Loader, B. (Eds.): *Cybercrime: Law enforcement, security and surveillance in the information age*, Routledge, London, 2000.

Tilley, N.: *Crime prevention*, Willan Publishing, Collumpton, 2009.

Turgeman-Goldschmit, O.: "Meanings that Hackers Assign to their Being a Hacker", en *IJCC*, vol. 2, julio-diciembre, 2008.

Tyler, T.R.: "Legitimacy and criminal justice: The benefits of self-regulation", en *OSJCL,* núm. 7, 2009.

Tyler, T.R.: *Why people obey the law*, Princeton University Press, Princeton, 2006.

Von Hirsch, A./Garland, D./Wakefield, A.: *Ethical and Social Perspectives on Situational Crime Prevention,* Hart Publishing, Oxford-Porltand, 2000.

Wall, D.: "Cybercrime and the culture of fear: Social Science fiction(s) and the production of knowledge about cybercrime", en *ICS*, vol. 11, núm. 6, 2008.

Wall, D.: *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge, 2007.

Wellman, B.: "Computer Networks As Social Networks", en *SM,* vol. 293, 14 de septiembre de 2001.

Wolak, J./Finkelhor, D. /Mitchell, K. J./Ybarra, M. L.: "Online "Predators" and their Victims: Myths, Realities and Implications for Prevention and Treatment", en *APs,* vol. 63, núm. 2, 2008.

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

Ybarra, M. L./Mitchell, K.: "Exposure to Internet Pornography among Children and Adolescents: A National Survey", en *CB,* vol. 8, núm. 5, 2005.

Young, R./Zhang, L.: "Factors Affecting Illegal Hacking Behavior", en *AMCIS 2005 Proceedings, p*aper 457, 2005, en Internet en http://aisel.aisnet.org/amcis2005/457. Citado el 3 de diciembre de 2010.

Yucedal, B.: "Victimization in cyberspace: An application of routine activity and lifestyle exposure Theories", 2010, en Internet en http://etd.ohiolink.edu/send-pdf.cgi/YUCEDAL%20BEHZAT.pdf?kent1279290984. Citado el 9 de agosto de 2011.

Zheng, R./Qin, Y./Huang, Z./Chen, H.: "Authorship Analysis in Cybercrime Investigation", en VV.AA.: *Lecture notes in computer science,* Springer Verlag, Berlin-Heidelberg, 2003.