INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual.

Prof. Dr. José R. Agustina Sanllehí
Profesor de Criminología y Derecho Penal
Universitat Internacional de Catalunya
e-mail: jragustina@uic.es

Abstract

Ante el avance de nuevas formas de delincuencia que se asocian al creciente aumento de usuarios en Internet, desde la Criminología se debe acometer el estudio de los factores criminógenos que facilitan la comisión de actos ilícitos. El espacio virtual genera una *atmósfera de anonimato* que protege, promueve y alimenta nuevos modos de atentar contra las personas e instituciones. Además, por la propia constitución de la red, las conductas delictivas adquieren una *potencialidad lesiva* que viene a multiplicar los posibles daños a terceros. En este sentido, resulta necesario profundizar y determinar las relaciones existentes entre (i) el modo de configurar los límites y las reglas que se aplican en ese espacio virtual y (ii) la consecuente atracción o generación de delincuencia que comporta. Sin embargo, las estrategias de prevención situacional topan con los límites derivados de la privacidad de los usuarios de Internet, la libertad de expresión y la libertad de navegación.

Palabras clave: *Ciber–delincuencia; delito informático. Políticas sobre restricciones en la libertad y privacidad en el uso de Internet y correo electrónico. Tecnología y delito. Prevención situacional del delito en espacios virtuales; delitos informáticos desde el lugar de trabajo. Globalización del delito.*

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

I. Introducción. La prevención situacional del delito en un entorno virtual: similitudes con los espacios reales y aplicabilidad de las teorías criminológicas tradicionales.

Con el creciente avance tecnológico, las nuevas plataformas de comunicación digital han experimentado con especial intensidad los efectos tanto positivos como negativos generados por la *globalización*. El espacio virtual de Internet constituye, sin duda, una *aldea global* en la que el entramado de redes y la proliferación de nodos repercuten de forma *inmediata* en las relaciones humanas. En este contexto, nos hallamos ante el reto de enfrentarnos a nuevos canales especialmente proclives para la comisión de delitos, a novedosas formas comisivas que, como se verá, poseen una mayor capacidad lesiva. Más aún, se puede llegar a afirmar que se ha iniciado una nueva etapa, distinta, en la lucha contra la delincuencia, caracterizada por lo que se viene denominando la *globalización del delito*.

Se ha señalado a este respecto que, en la medida en que se incrementa de forma progresiva el acceso y la utilización de Internet, aumenta la preocupación por el uso inadecuado de tales formas de comunicación (*Newburn*, 2007: 104). De este modo, el término con que se designan las nuevas formas de delincuencia, «*cybercrime*», ha pasado a ocupar un lugar habitual en nuestro lenguaje cotidiano. Y en tal contexto, Internet deviene uno de los instrumentos principales en la tendencia apuntada.

Los nuevos *ciberdelitos* han sido así definidos como «aquellas actividades mediadas por el uso de ordenadores que son ilegales o se consideran ilícitas por parte de terceros y que pueden llevarse a cabo a través de redes electrónicas de alcance global» (*Thomas & Loader*, 2000: 3).

Sin embargo, en el contexto de la prevención del delito, la naturaleza del *espacio real* y del *espacio virtual* guardan, en realidad, innegables semejanzas. Así, la imagen gráfica del efecto que pueden tener unas *ventanas rotas («broken windows»)* en la degradación paulatina del orden y del control de la delincuencia en el entorno de un determinado barrio, se puede aplicar –*mutatis mutandis*– al desorganizado *espacio virtual* que, en la actualidad, constituye Internet. En este sentido, resulta necesario profundizar y determinar las relaciones existentes entre (i) el modo de configurar los límites y las reglas que se aplican en ese espacio virtual y (ii) la consecuente atracción o generación de delincuencia que comporta.

En los últimos años, gran parte de la investigación sobre la delincuencia en el espacio real (*realspace*) relativa a aquellos indicadores del entorno que generan delincuencia se ha asociado a la conocida teoría criminológica de James Q. WILSON y George L. KELLING, «the broken windows theory»[1]. Según esta teoría, en el ámbito del control de la delincuencia deben corregirse y/o castigarse los *desórdenes visibles* –

[1] KELLING, G.L., COLES, C.M. (1996). Para una comprensión sucinta de la *teoría de las ventanas rotas* y su impacto en el desarrollo de la Criminología actual, *vid*. MCLAUGHLIN, E., MUNCIE, J. (2007), pp. 27–29.

aunque éstos sean de menor escala– porque pueden llegar a tener el efecto negativo de engendrar mayor desorden y, con frecuencia, mayor delincuencia. De este modo –se argumenta al respecto–, se considera más eficaz dedicar mayores recursos a la persecución y control de aquellos desórdenes y delitos menos graves[2]. Es decir, el hecho de no aplicar medidas correctoras ante lo que parece *insignificante* tiene la capacidad de transmitir, en este sentido, un mensaje ciertamente negativo («*disorder is tolerated*»), que conduce –mediante una pendiente resbaladiza– a una peligrosa *reacción en cadena* («*petty disorderly acts, which are not necessarily breaches of the criminal law, trigger a chain reaction that undermines community safety*»)[3].

Aplicando las anteriores consideraciones al *espacio virtual*, KAYTAL señala con acierto que:

> «hoy en día el ciber–espacio es oscuro. No se puede ver qué están haciendo el resto de usuarios en un momento dado. Sin embargo, en la medida en que la preocupación por el delito informático va en aumento, la arquitectura podría suponer un giro repentino –del mismo modo a como sucedió con la irrupción de la luz de gas y la electricidad– y arrojar así luz sobre los usuarios en el ciber–espacio»[4].

[2] KATYAL, N.K. (2002), p. 117, donde apunta que, por otra parte, la prevención del *cybercrime* a través de la ley y de un diseño arquitectónico público del espacio en la red puede impedir los intentos de restringir las libertades relacionadas con Internet por parte de agentes privados (vid., p. 117).
[3] *Vid.* MCLAUGHLIN, E., MUNCIE, J. (2007), p. 28.
[4] «… [T]oday cyberspace is *dark*. One cannot see what other users are doing at any given time. But, as concern about computer crime becomes greater, the architecture could flip—just as it did with the advent of gas lighting and electricity—and shed light on users in cyberspace» (KATYAL, N.K. (2002), p. 116).

Mediante el recurso analógico a la iluminación como un factor sutil de incidencia en el entorno criminológico, argumenta que se deberían promover aquellas condiciones que tengan efectos positivos respecto de los índices de criminalidad en un espacio determinado.

En tal contexto, nos proponemos realizar algunas consideraciones de utilidad sobre las particularidades y nuevos desafíos que, desde el punto de vista criminológico, suponen las nuevas tecnologías en la sociedad actual. No obstante, conviene apuntar que, desde los primeros momentos en que surgió Internet, se ha planteado un intenso debate entre (i) quienes abogan por la necesidad de prevenir y sancionar los malos usos en la red, por los efectos criminógenos asociados, y (ii) quienes defienden que ciertas áreas deben quedar libres de intervencionismo, decantándose por la protección del derecho a la intimidad y de la libertad de expresión[5].

II. Tecnología y delito: unas relaciones de interacción complejas.

En realidad, la novedad que supone el espacio virtual de Internet, el uso de correo electrónico y otros instrumentos tecnológicos, así como su posible utilización para fines delictivos (*side effects*), se inscribe en la poderosa interacción entre

[5] *Vid.* RIBAS ALEJANDRO, J. (2003), p. 127.

tecnología y *delincuencia* descrita desde el ámbito de la sociología de la delincuencia[6]. A este respecto, la pregunta que se plantea ante las nuevas formas de comisión delictiva, *¿cómo interactúan cultura y tecnología en los cambios sociales y en las tendencias delictivas?*, ha encontrado respuestas aparentemente opuestas.

Siendo crítico con los planteamientos de las «teorías de la estructura social» –teorías que ponían el énfasis en las normas y desigualdades sociales como *factor de cambio*–, William F. OGBURN (1964)[7] sostuvo a este respecto que, en realidad, son los cambios tecnológicos los que tienden a conducir los cambios en la sociedad. Ciertamente, las tesis de OGBURN no tuvieron aceptación en el entorno académico en el que surgieron. Sin embargo, a pesar de lo discutibles que puedan parecer sus tesis, Marcus FELSON mantiene que la descripción sociológica que efectúa OGBURN sugiere una importante lección en el ámbito criminológico, cual es, que debemos dejar de asumir que los cambios en la delincuencia vendrán por los cambios introducidos en la cultura. Sin negar que ésta tenga relevancia, afirma en este sentido que la tecnología es, en última instancia, la principal fuerza conductora de las transformaciones sociales y, por tanto, los cambios tecnológicos son los que provocan alteraciones en las formas de delincuencia –siguiendo la cultura la estela de tales cambios tecnológicos–[8].

[6] Para un acercamiento a las raíces sociológicas del problema *vid.* FELSON, M. (1997), pp. 81–96.
[7] OGBURN, W.F. (1964).
[8] *Vid.* FELSON, M. (1997), pp. 82–83.

La teoría de OGBURN se explica a partir del concepto acuñado por él mismo, denominado «cultural lag». La idea es simple: según su descripción, primero se produce un cambio en la tecnología y, posteriormente, tras un cierto período de tiempo, tiene lugar un cambio en la cultura. En este sentido, cualquier elemento presente en la cultura que no sea útil o práctico para el estado actual del desarrollo tecnológico se denomina «cultural lag»[9]. Así, una persona de negocios que trabajando en París todavía se desplaza a su casa al mediodía para comer refleja un retraso cultural. El tráfico es demasiado denso y resulta poco práctico invertir en el desplazamiento, aunque algunos así lo hagan. Hasta en París la cultura del *fast–food* se expande. El colapso de la circulación fuerza un cambio en el comportamiento de la gente, pasando por encima de la cultura misma[10].

Marcus FELSON describe el proceso y explica el porqué de la importante relación de la tecnología en la empresa y sus implicaciones criminológicas. Establece relaciones entre la anteriormente descrita teoría de ORGBUN y la *sociología de la invención*, de GILFILLAN (1970). Utiliza el concepto de paradigma de KUHN (1970) y la descripción del funcionamiento de las organizaciones complejas de Max WEBER (1922). Y concluye con la teoría de la ecología humana de Amos HAWLEY (1950). La tecnología es así la

[9] *Cultural lag* podría traducirse como un retroceso o atraso cultural, un *anacronismo* respecto de las pautas culturales del momento.
[10] FELSON, M. (1997), p. 82.

herramienta idónea, más eficaz, en el proceso de adaptación de organizaciones complejas, de grandes dimensiones. Mediante el aprendizaje en el modo de usar las nuevas tecnologías se establecen vínculos de interdependencia entre los miembros de una empresa –o de una comunidad en general–. De esta forma, se facilita la adaptación del individuo al entorno y se generan procesos de simbiosis, cooperación, competitividad y depredación[11].

Si bien los cambios tecnológicos están llamados a impregnar todas las capas de la sociedad, la empresa es el principal motor que impulsa la innovación tecnológica y, en ese sentido, viene a ser un espacio privilegiado donde van a concurrir nuevas oportunidades delictivas y nuevos sistemas de prevención[12]. Sin embargo, el correo electrónico no puede considerarse sólo como un potencial *instrumento delictivo*. Las herramientas de trabajo en la *era tecnológica* –la utilización del e–mail por parte de los trabajadores, como cualquier otro canal de comunicación social– deben ser analizados desde una doble dimensión: (1) por un lado, permiten la comisión de delitos, sirviendo de algún modo su estructura o espacio de comunicación como *medio comisivo* o *herramienta de preparación o concertación delictiva* y, (2) por otro, facilitan su

[11] *Vid*. GILFILLAN, S.C. (1970); KUHN, T.S. (1970); WEBER, M. (1922); HAWLEY, A. (1950); FELSON, M. (1997, pp. 82–83).
[12] Véase, al respecto, AGUSTINA SANLLEHÍ, J.R. (2009), *Límites en las estrategias de prevención del delito en la empresa. A propósito del control del correo electrónico del trabajador como posible violación de la intimidad*, InDret 2/2009 (disponible en Internet en www.indret.com).

prevención e investigación, en cuanto mecanismo de control del empresario o de investigación de la justicia.

Las nuevas tecnologías tal vez no introduzcan *elementos nuevos* en los rasgos esenciales de las tradicionales categorías y tipos delictivos. Por el contrario, la novedad de la *ciber–delincuencia* reside más bien en los nuevos modos de delinquir, la multiplicación de los efectos lesivos y las nuevas formas de prevención e investigación. Las nuevas tecnologías suponen así un ámbito adicional de aplicación de las teorías de *prevención situacional del delito*. De este modo, con el fin de *prevenir*, *controlar* e *investigar* la realidad delictiva en la empresa resulta especialmente conveniente estudiar adecuadamente el modo de organizar y estructurar el uso de las nuevas tecnologías por parte de los trabajadores.

Respecto de estas nuevas realidades tecnológicas se puede aplicar el enfoque criminológico descrito por la «teoría de la oportunidad delictiva» (*Cohen* y *Felson* 1979). Así, con el fin reducir en lo posible las ocasiones delictivas, conviene fijar la atención en las características del *objetivo* delictivo determinado. A la luz de las consideraciones de COHEN y FELSON, se puede afirmar que (1) el *valor* de los *objetivos* para posibles delincuentes se multiplica, al ritmo de las nuevas invenciones y de la producción masiva de productos en la sociedad de consumo; (2) la *inercia* o la resistencia que dificulta el movimiento de los objetivos (virtuales) aminora o

desaparece, facilitándose la comisión delictiva (*lightweight targets*); (3) la *visibilidad* y (4) el *acceso* al objetivo, en tanto que la tecnología se expande a todas las esferas de la sociedad, tienen también un efecto multiplicador de las *tentaciones* y *oportunidades* delictivas.

III. Elementos relevantes en el diseño de la arquitectura digital: barreras cognitivas, control, transparencia.

Como se señaló en nuestras investigaciones precedentes, la prevención de cualquier clase de delitos requiere no sólo una *respuesta normativa* sino también una *reacción cognitiva*. Así, para luchar eficazmente contra la delincuencia informática –por ej., la pornografía infantil a través de la red–, además de establecerse los medios normativos pertinentes que criminalicen las conductas y permitan una persecución e investigación más allá de los límites de un único Estado, deberían aumentarse los mecanismos de transparencia y control en la navegación por Internet, estableciéndose un principio de *privacidad limitada*. Sin duda, el establecimiento de determinadas reglas del juego por las que se conciencia a los usuarios de que la navegación puede ser investigada en caso de necesidad, y la reducción de posibilidades de permanecer en el anonimato tienen un enorme efecto disuasorio en los delitos cometidos a través de la

red. Tales posiciones entran en conflicto, no obstante, con el pretendido derecho a la *privacidad absoluta* en el uso de Internet[13].

De nuevo la tensión entre libertad [privacidad] *versus* seguridad [prevención] en el centro del discurso que propone intensificar el control de riesgos delictivos. En este caso, la libertad de navegar por la red, libre de controles, sin necesidad de identificación alguna, frente a la presencia de puntos peligrosos en Internet, connaturales a un espacio donde el anonimato tiene claros efectos criminógenos. En este sentido, la red es –dentro de la tipología de lugares acuñada por *Brantingham* y *Brantingham* (1995)– tanto un lugar criminógeno, en el sentido de que por sus mismas condiciones genera delincuencia (*crime–generators*), como un espacio propicio que atrae al delincuente a cometer sus delitos (*crime–attractors*), en el que existen menores *riesgos* y abundan distintos *objetivos*[14].

Parece razonable objetar a una pretensión ilimitada de navegar libremente –gozando de una privacidad de carácter *absoluto*– la necesidad de poner ciertos límites, controles o sistemas de identificación en aquellos sitios–web donde existan riesgos estadísticos de cometerse fraudes o de ser punto de ignición del abuso de menores u otra clase de delitos (*hot–spots*). Sin duda, un mayor control puede aminorar la atracción y

[13] *Vid.* en general CASTELLS, M. (2003).
[14] ECK, J.E. (1997), p. 130.

generación de delincuencia, sacrificando –o más bien *limitando*– algunas prerrogativas de privacidad de las personas.

Una de las medidas cognitivas posibles que dificultan o imposibilitan la comisión de delitos consiste en adaptar con fines preventivos la disposición y el diseño del contexto espacial en el que se encuentran los bienes jurídicos que se desean proteger. En este sentido la arquitectura digital puede operar como un límite cognitivo al comportamiento *online* del trabajador. Tales medidas se proponen actuar sobre el entorno de forma eficaz, reduciendo las oportunidades del delito.

Los rasgos y la caracterización del entorno físico de los edificios se comenzaron a percibir como un factor «intrínsecamente criminógeno» y por tanto, un elemento significativo en el marco de la prevención situacional del delito a partir de 1920[15]. Así, la implementación de medidas en el diseño y disposición arquitectónica del entorno se empezó a concebir como un instrumento idóneo para reducir la criminalidad y proteger a las comunidades poblacionales, tanto en espacios públicos como privados[16]. La comparación analógica entre la inseguridad que pueda haber en las calles y la que tiene lugar en el espacio digital irá cobrando una mayor relevancia, especialmente a medida

[15] *Vid.* en general JACOBS, J. (1961); NEWMAN, O. (1972).
[16] Las investigaciones que empezaron a realizarse a partir de 1920 en la Universidad de Chicago llevaron a la conclusión de que era la naturaleza y el particular diseño de determinados barrios, y no el tipo de población, lo que determinaba la persistencia de altos índices de criminalidad, a pesar de los frecuentes cambios poblacionales (*vid.* MCLAUGHLIN, E., MUNCIE, J. (2007), p. 115).

que la generalización en el acceso y uso de la red se expanda a todas las capas de la población[17].

«*To prevent crime, governments and citizens must devote far more attention to the positive and negative consequences of architecture*»[18]. En tanto que la prevención del delito no puede infravalorar los efectos positivos y negativos que puede tener el entorno en los índices de criminalidad, KAYTAL analiza la arquitectura digital en el marco del control del delito[19], sugiriendo los siguientes principios en el diseño digital en relación a los fines de prevención del delito.

En primer lugar, (1) se debe fomentar una vigilancia natural en el entorno *(natural surveillance*). Siguiendo a Jane JACOBS, argumenta que si la visibilidad en el diseño de las manzanas en que se dividen las ciudades disminuye los índices de criminalidad (*eyes on the street would control crime*), se debería fomentar una mayor transparencia en la red, en la programación, en los mecanismos existentes de control[20]. Por tanto, los espacios cerrados pueden incrementar la realización de delitos. La privacidad y el anonimato, la configuración del *software* como una realidad de acceso restringido, el empleo de códigos de acceso y en general la creación de comunidades

[17] *Vid.* KATYAL, N.K. (2002), p. 103. Téngase en cuenta que es ciertamente bajo el nivel de familiarización y uso de las nuevas tecnologías por parte de la población reclusa.
[18] He aquí el punto de partida de KATYAL, N.K. (2002), pp. 128.
[19] KATYAL, N.K. (2002), pp. 104–128.
[20] Obsérvese que las características de la prevención del delito en el ciberespacio, al realizarse generalmente de forma no visible, reducen las consecuencias positivas en la prevención que se derivan de la vigilancia natural.

cerradas (*gated communities*), ya sea en el espacio real o virtual, tiene efectos contraproducentes: respondiendo a una lógica del miedo al delito no aportan en ocasiones más que una falsa sensación de seguridad.

A este respecto, junto a los grandes avances y las enormes posibilidades de progreso que ha supuesto Internet, conviene advertir, no obstante, sus efectos negativos. Internet, al igual que otros medios de comunicación, no está exento de la necesidad de establecer leyes razonables que se opongan a las palabras de odio, a la difamación, al fraude, a la pornografía infantil –a la pornografía en general, en cuanto instrumento de explotación de la mujer–, y a otras desviaciones. La conducta delictiva en otros contextos es también conducta delictiva en el ciberespacio, y los poderes públicos tienen el deber y el derecho de hacer cumplir las leyes.

Sin embargo, la mentalidad opuesta a cualquier tentativa de reglamentación por parte de la responsabilidad pública ha estado presente de algún modo desde sus inicios con respecto a Internet. Cualquier cortapisa a la libertad de expresión, cualquier límite a la estructura descentralizada y desorganizada, se consideraba contraria al espíritu de los defensores a ultranza de que la única ley fuera la completa libertad de hacer cada uno lo que le pareciera. Por supuesto, esto significaría que la única comunidad cuyos derechos e intereses se deben reconocer en el ciberespacio sean los de la comunidad de aquéllos, partidarios de una libertad sin límites. Este modo de pensar está en la base de una

defensa de la pornografía y de la violencia en los medios de comunicación en general. Aunque los individualistas radicales y los empresarios constituyen obviamente dos grupos muy diferentes, hay una convergencia de intereses entre quienes buscan que Internet se convierta en un lugar apto para cualquier tipo de expresión –sin importar su contenido, si es vil o destructivo–, y quienes quieren que sea un vehículo de actividad sin trabas según un modelo neoliberal que «considera las ganancias y las leyes del mercado como parámetros absolutos, en detrimento de la dignidad y del respeto de las personas y los pueblos»[21].

Muchas cuestiones difíciles con respecto a Internet requieren el consenso internacional: por ejemplo, cómo garantizar la privacidad de las personas y los grupos que observan la ley, sin impedir que se aplique la ley y permitiendo que el personal de seguridad vigile sobre delincuentes y terroristas[22].

En este sentido, el uso del correo electrónico laboral se puede concebir como un instrumento de comunicación de la *comunidad empresarial*, en un contexto de relativa transparencia que se fundamenta en el trabajo en equipo. Un planteamiento abierto de las comunicaciones en la empresa reduciría *de forma natural* las expectativas de privacidad, expectativas que se vienen a generar cuando, de hecho o de derecho, por la propia configuración del sistema, se construyen ciertos espacios de comunicación como

[21] *Cfr.* JUAN PABLO II, *Ecclesia in America*, n. 56.
[22] *Vid.* al respecto, Pontificio Consejo para las Comunicaciones Sociales, «Ética en Internet» (2002).

ámbitos cerrados y excluyentes frente a terceros, siendo tal exclusividad un derecho con aspiración a no admitir excepciones.

Una segunda técnica de prevención del delito –continúa KAYTAL– se basa en (2) la *territorialidad*. Construir escenarios y edificios que pongan de manifiesto la territorialidad, el sentido de que se visualiza la propiedad sobre un área determinada (*a signal of stewardship o fan area*), ejerce de contrapeso a la disposición abierta del entorno, viniendo a facilitar una *vigilancia natural* –anteriormente mencionada–[23]. La configuración de las puertas de acceso al sistema (*log in*), en este sentido, define un territorio, permite el acceso al mismo y coadyuva en la identificación del usuario *ex post facto*. La territorialidad en el *espacio real* permite reconocer a los intrusos e intervenir a tiempo. Sin embargo, el reconocimiento de intrusos en el ciberespacio viene dificultado por el hecho de que los protocolos de Internet se basan en líneas generales en un «principio de no identificación del usuario». De hecho, una de las principales razones por las que Internet es un campo fértil para la aparición del delito es la generación de una «expectativa de anonimato»[24]. A pesar de ello, el modo de identificación genérico en la red mediante el *«Internet Protocol logging»* (IP) puede facilitar en muchos casos

[23] Si el espacio se configura *demasiado cerrado*, se imposibilita la vigilancia natural por parte de terceros, mientras que si se construyen espacios *excesivamente abiertos* se promueve la intrusión y el delito (*vid.*, KATYAL, N.K. (2002), p. 108).

[2424] *Vid. Doe v. 2TheMart.com*, Inc., 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001), sobre una conversación anónima en un *chat* que supuestamente dio una visión alejada de la realidad de la conducta de la empresa y que arruinó el valor en Bolsa de la compañía. En realidad, aunque se presuma un derecho al anonimato no se trata más que, en cierto modo, el equivalente digital al mecanismo de cubrirse el rostro que emplea quien atraca un banco.

el seguimiento de la pista del delito –normalmente después del hecho–, aunque no siempre con resultados plenamente satisfactorios, en tanto que los delincuentes más sofisticados pueden enmascarar su verdadera identidad mediante una gran variedad de técnicas[25].

En tercer lugar, (3) describe el principio denominado *«building communities»*, mediante el que se pretenden potenciar los diseños arquitectónicos que faciliten la interacción y promuevan la reciprocidad. En determinadas formas de delincuencia, el uso de la arquitectura en ese sentido puede resultar un medio eficaz para detectar y evitar en tiempo real la comisión de un delito. Así, los miembros de una comunidad virtual pueden intervenir ante ciertas formas de acoso *online*. Sin embargo, en la mayoría de los delitos que tienen lugar en la red –piratería, accesos no autorizados, pornografía infantil– éstos no son visibles en absoluto al resto de sus iguales[26].

En último lugar, KAYTAL se refiere a (4) la limitación en la protección a objetivos determinados (*target proteccion*), como un medio efectivo que evite una excesiva implementación de instrumentos de prevención y control. Los efectos negativos de una tendencia excesiva en esta línea entre la población podría conducir a la

[25] KATYAL, N.K. (2002), p. 109.
[26] *Cfr.* KATYAL, N.K. (2002), p. 116.

«fragmentación de la comunidad», es decir, a la ruptura de los vínculos recíprocos en base a una desconfianza generalizada[27].

IV. Prevención del delito informático *desde el lugar de trabajo*.

Junto a las propuestas relativas a la reconfiguración *general* del *campo de juego* que constituye Internet, no se puede ignorar que (i) buena parte de los usuarios sólo acceden a la red *a través de los instrumentos de trabajo*; y que (ii) el tiempo relativo de navegación y utilización de las tecnologías de la comunicación desde el lugar de trabajo supera, las más de las veces, con mucho, al tiempo de acceso desde herramientas informáticas privadas. Por ello, intervenir sobre las herramientas que pertenecen a la empresa debería ser considerado uno de los factores ambientales sobre los que se puede incidir de una forma más asequible y con menor afectación a la privacidad del usuario.

La criminalidad en el contexto empresarial posee particularidades propias que conviene tener presente. Como pusieron de manifiesto Marcus FELSON y Ronald CLARKE (1997), «*something new is needed to bridge this gap*», en referencia al escaso interés prestado hasta el momento por la literatura criminológica en el estudio de la

[27] *Vid.* KATYAL, N.K. (2002), p. 119 y ss. Uno de los argumentos liberales que acostumbra a minusvalorarse en relación a la función de control del delito que ejercen las fuerzas de seguridad del Estado radica precisamente en que cultiva y protege los lazos entre la comunidad (*vid.* p. 120). Sin embargo, el hecho de que sea desde el Estado o desde la seguridad privada desde donde se genere un tal clima social de desconfianza no modifica *per se* la situación –así, el ejemplo citado relativo a que el miedo a las interceptaciones puede llevar a muchos a tener miedo a usar el correo electrónico puede aplicarse tanto a un control estatal como empresarial–.

relación entre *delito* y *empresa*. El nacimiento de un nuevo campo de investigación empírico en torno a la criminalidad en la empresa ha comenzado a despertar interés tanto desde el sector público, como desde el propio ámbito empresarial, sin duda por la conciencia cada vez mayor de las repercusiones de este tipo de delincuencia en la economía de la empresa y en el progreso de la sociedad[28].

Se pueden enumerar diferentes razones por las que no conviene en absoluto despreciar la relevancia del entorno laboral para el análisis criminológico y criminógeno de la persona y su entorno (*ofender/context relationship*)[29]. En términos comparativos, el lugar de trabajo puede considerarse el contexto de relación en el que la persona adulta se desenvuelve durante más tiempo. En este sentido, es en el contacto diario con su entorno laboral y la cultura imperante en su lugar de trabajo donde el individuo adopta con facilidad –en ocasiones imperceptiblemente– pautas de conducta moralmente adecuadas o por el contrario desviadas. Tales referencias de valores se interiorizan de tal forma que pueden llegar a tener consecuencias difíciles de cuantificar aunque no por ello menos intensas y decisivas. El lugar de trabajo es, en este sentido, un significativo *medio de socialización* y de interiorización de códigos de conducta. Por otro lado, las particularidades y rasgos propios que caracterizan una profesión u oficio imprimen un

[28] *Vid.* FELSON, M., CLARKE, R.V., *Business and Crime Prevention*, 1997, pp. 1–3, en donde justifican el interés objetivo por ese estudio: «crime is an essential topic for business because it threatens profits while interfering with business goals and relations to a larger society».
[29] WILLISON, R., *Understanding the perpetration of employee computer crime in the organizational context*, Information and Organization 16 (2006) 304–324.

influjo considerable en la personalidad del individuo, en sus hábitos de conducta y en sus precomprensiones, que pueden posteriormente manifestarse en una carrera delictiva.

Desde un punto de vista criminógeno, la ausencia de vínculos de integración social del trabajador respecto de la empresa, su falta de identificación con la compañía, la carencia de motivaciones positivas desde el punto de vista psicológico o emocional pueden considerarse una causa de su comportamiento delictivo. La empresa no deja de ser una comunidad de personas, *una sociedad dentro de una sociedad* en la que a escala menor se aplican las teorías de los vínculos sociales (*social bond theories*). La importancia de los lazos personales e institucionales explica –de acuerdo con tales teorías– por qué algunos individuos cometen delitos mientras que la mayoría no lo hace[30].

DAVIES y JUPP sostuvieron ya a finales de los noventa que las conexiones entre *delito* y *trabajo* habían sido sólo parcialmente examinadas en el ámbito de la Criminología[31]. Aunque en años posteriores hemos asistido a un creciente interés por analizar las causas y proponer soluciones preventivas al delito dentro de la empresa, la escasa investigación empírica y el menor interés criminológico en torno a los delitos en el lugar de trabajo (*crime at work*) sigue siendo significativa, especialmente si se tiene

[30] BUSSMANN, K.–D., *Causes of Economic Crime and the Impact of Values*, 2003, p. 10.
[31] DAVIS, P., FRANCIS, P., JUPP, V., *Crime–Work Connections: Exploring the 'Invisibility' of Workplace Crime*, in DAVIS, P., FRANCIS, P., JUPP, V., Invisible Crimes. Their Victims and their Regulation, 1999, pp. 55.

en cuenta la relevancia del nivel de pérdidas económicas que suponen, en líneas generales, tales tipos de delitos para el conjunto de la economía.

Como señalan RICKMAN y WITT, las investigaciones sobre las relaciones existentes entre *actividad económica* y *comportamiento criminal* deberían centrarse en el abordaje de los *factores determinantes* o que pueden favorecer la comisión de delitos por parte de los trabajadores[32]. Si bien tratar de establecer tales factores determinantes de la delincuencia no permite reducir el comportamiento de los agentes implicados a variables econométricas, una aproximación al fenómeno delictivo desde la lógica económica y en el contexto empresarial puede aportar, más que en otros ámbitos, ciertas orientaciones esclarecedoras sobre las causas y la fenomenología delictiva[33].

Nick J. DODD viene a identificar dos perfiles característicos del trabajador que comete un delito en la empresa, a partir del estudio de CCD (*Corporate Crime Data Sample*): el empleado problemático que genera problemas y aquél que *no tienen nada*

[32] RICKMAN, N. and WITT, R., *The Determinants of Employee Crime in the UK*, Economica (2007) 74, p. 172. En este artículo analizan los resultados de un estudio empírico realizado, en el que se ha trabajado con un concepto extensivo de *'employee crime'*, abarcando el uso deliberado de los bienes del empresario en provecho personal del trabajador (ya se trate de hurtos de productos de la empresa, fraudes financieros o el uso no autorizado de equipos de la empresa para actividades no relacionadas con la prestación laboral): *vid.* p. 161.

[33] La sociología del delito trata de establecer *correlaciones causales*. La psicología del delito, *motivaciones personales*. Ambas perspectivas pretenden *explicar* el fenómeno delictivo desde su perspectiva propia, pero ambas se topan en último término con la libertad humana como *factor inexplicable*. Lo que quiere señalarse es que, en el intento de hallar una explicación a *por qué surge el delito*, tal vez las variables econométricas y el cálculo económico tengan un mayor peso en el contexto de la empresa que, por ejemplo, en delitos sexuales o delitos contra la seguridad viaria. Mayor o menor peso no excluye que la posición económica del delincuente pueda tener cierta relevancia en el momento de realizar *cualquier* delito.

que perder: «'Troublemaker' and 'Nothing to Lose' employee offenders»[34]. En este sentido, una importante fuente de información sobre el sujeto individual puede proceder del estudio de datos reales. Aunque algunos factores ya han sido objeto de investigación con cierta profundidad, tales como el género (*Jones*, 1972; *Moretti*, 1986; *Terris*, 1985), edad y estabilidad en el puesto de trabajo (*Franklin*, 1975; *Hollinger y Clark*, 1983; *Hollinger et al.*, 1992; *Robin*, 1969; *Robertson*, 1993), presión económica (*Dodd*, 1998; *Cressey*, 1953), *status* (*Greenberg*, 1990; *Laird*, 1950; *Szwajkowski*, 1989; *Tucker*, 1989), confianza (*Cressey*, 1953; *Harrell y Hartnagel*, 1976; *Hollinger y Clark*, 1983; *Paul*, 1982), integración o arraigo (*Ditton*, 1977; *Hollinger*, 1986; *Hollinger and Clark*, 1983; *Mars*, 1974; *Murphy*, 1993), rasgos de la personalidad (*Murphy*, 1993; *Paajanen*, 1988), no obstante, resulta difícil separar con nitidez y afirmar con determinación qué aspectos de tales factores que describen el perfil criminológico del trabajador proceden de los resultados de la investigación empírica disponible. Concretamente, la validez y fiabilidad de los rasgos de la personalidad ha sido puesta en entredicho debido a su falta de consistencia en el tiempo y el carácter temporal de ciertas actividades desviadas (*Sackett*, 1985; *Sackett y Harris*, 1985)[35].

---

[34] *Cfr.* al respecto, DODD N.J., *'Troublemaker' and 'Nothing to Lose' Employee Offenders Identified from a Corporate Crime Data Sample*, Crime Prevention and Community Safety: An International Journal 2004, 6 (3), 23–32; *vid.* también, el estudio llevado a cabo por SPEED, M., *Reducing Employee Dishonesty: In Search of the Right Strategy*, in Managing Security. Crime at Work (Volume III), Leicester, 2003, Chapter 10, pp. 157–179.

[35] DODD N.J., *Ibid.*, 2004, pp. 24–25. Una de sus tesis consiste en que no se puede distinguir al trabajador que delinque del resto de sus compañeros de trabajo que no muestran comportamientos desviados.

Así, siguiendo un nuevo modo de aproximarse a la realidad del delito mediante un enfoque económico, introducido por primera vez por BECKER (1968)[36], los economistas se comenzaron a interesar por el estudio del comportamiento criminal, pero sin prestar demasiada atención en un primer momento a los delitos de los trabajadores (*employee crime*)[37]. Posteriormente, BARNES y LAMBELL (2002) realizaron por vez primera un estudio en el ámbito de la criminalidad en la empresa, en el que se introducía la metodología propia de la Econometría[38]. Sin embargo, su trabajo se fundamentó exclusivamente en las percepciones procedentes de las organizaciones empresariales, restando por tanto fiabilidad a las conclusiones obtenidas. No es hasta la reciente investigación llevada a cabo por RICKMAN y WITT (2005), cuando se empieza a trabajar empleando datos procedentes de los delitos registrados en el seno de las empresas –en su estudio, limitado al Reino Unido–. Su trabajo de campo aporta una información extraída directamente de la realidad, abarcando datos sobre los hurtos cometidos por los trabajadores, las políticas que pueden ayudar a combatirlos y los puntos de vista alternativos sobre las distintas motivaciones para cometer el delito[39]. Finalmente,

[36] BECKER, G., *Crime and punishment: an economic approach*, Journal of Political Economy, 76, (1968), pp. 169–267.
[37] DICKENS, W.T., KATZ, L.F., LANG, K., SUMMERS, L.H., *Employee crime and the monitoring puzzle*, Journal of Labour Economics, 7, (1989), pp. 331–347.
[38] BARNES, P., LAMBELL, J., *Organisational Susceptability to Fraud: Does Fraud Strike Randomly or Are There Organisational Factors Affecting its Likelihood and Size?*, Working Paper, Nottingham Business School, (2002).
[39] RICKMAN, N. AND WITT, R., *The Determinants of Employee Crime in the UK*, Economica (2007) 74, p. 161.

BUSSMANN y WERLE (2006) dan un paso más y realizan el primer estudio del delito en la empresa de carácter transnacional.

La investigación de BUSSMANN y WERLE se lleva a cabo mediante una encuesta global a más de 5.500 empresas, combinando información sobre las propias compañías, su victimización y sobre el descubrimiento y resolución de 2.900 incidentes relativos a este tipo de delitos[40]. La relevancia del estudio se debe en gran medida al ámbito mundial de la encuesta y al volumen de la muestra de datos en los que se basa, revelando como resultado ciertos rasgos comunes en la perpetración y victimización del delito en la empresa, así como ciertas pautas homogéneas también en los *modus operandi* registrados.

Desde una perspectiva más directamente encaminada al objeto de análisis, en el ámbito español, *Landwell & Pricewaterhouse Coopers* ha presentado un informe bajo el título «Actos desleales de trabajadores usando sistemas informáticos e Internet»[41]. Entre

[40] BUSSMANN, K.–D., WERLE, M. M., *Addressing Crime in Companies. First Findings from a Global Survey of Economic Crime*, British Journal of Criminology (2006), 46, pp. 1128–1144.

[41] De forma similar a los CCD, la finalidad principal del estudio es obtener conclusiones sobre los tipos de infracciones que se cometen con más frecuencia, la estrategia seguida por las empresas, el porcentaje de casos a los que se llega a un acuerdo, los sectores más afectados, las motivaciones que hacen que los trabajadores actúen de esta manera, la cuantía de los daños y la evolución cronológica de las infracciones. El estudio se realizó a partir del análisis de 393 casos en empresas españolas, desde el 1 de enero de 2001 hasta el 31 de diciembre de 2003 (*vid.* «Actos desleales de trabajadores usando sistemas informáticos e internet», Informe elaborado por Landwell–PwC, dirigido por Javier RIBAS, responsable del Departamento de Derecho de las Tecnologías de la Información, *Relaciones Laborales*, núm. 21, Año XX, Quincena del 8 al 23 Nov. 2004, p. 1317, Tomo 2, *Editorial La Ley* (LA LEY 2355/2004).

las conclusiones, se presenta –de forma similar a los *Corporate Crime Data* (CCD)[42]– un cuadro con las infracciones más habituales, acompañado de una descripción de algunos elementos más comunes relativos a la génesis y fenomenología del *employee crime*, tales como el *modus operandi*, las motivaciones del trabajador o las situaciones que han facilitado la comisión del delito o infracción. Al tratarse de un *listado de infracciones*, no recoge conductas delictivas en sentido estricto, aunque en la práctica la línea divisoria entre *delito, infracción e irregularidad* presenta contornos difusos[43]:

(1) *Creación de una empresa paralela, utilizando activos inmateriales de la empresa*

Consiste en la explotación en una empresa de nueva creación, de la propiedad intelectual, la propiedad industrial o el *know how* de la anterior empresa. Generalmente, el trabajador constituye la nueva compañía antes de solicitar la *baja voluntaria* y realiza un proceso de trasvase de información mediante soportes informáticos o a través de Internet. Es posible que el trabajador actúe de forma conjunta con otros compañeros de la empresa. Los hechos pueden tener

[42] RICKMAN, N., WITT, R., *The Determinants of Employee Crime in the UK*, Economica (2007) 74, p. 172, donde cita los estudios de BARNES, LAMBELL: *vid.* BARNES, P., LAMBELL, J., *Organisational Susceptability to Fraud: Does Fraud Strike Randomly or Are There Organisational Factors Affecting its Likelihood and Size?*, Working Paper, Nottingham Business School, (2002).

[43] BLOUNT, E.C., *Occupational Crime*, 2003, p. 4, donde se refiere a un concepto multidimensional de «occupational crime» como comportamiento abusivo del trabajador para abarcar el problema en toda su naturaleza.

relevancia penal a la luz del artículo 278 CP (*descubrimiento y revelación de secretos de empresa*).

(2) *Daños informáticos y uso abusivo de recursos informáticos*

Los daños informáticos se producen generalmente como respuesta a un conflicto laboral o a un despido que el trabajador considera injusto. Consisten en la *destrucción, alteración o inutilización* de los datos, programas o cualquier otro activo inmaterial albergado en redes, soportes o sistemas informáticos de la empresa. Los casos más habituales reflejados en el informe son los virus informáticos, el sabotaje y las *bombas lógicas*, programadas para que tengan efecto unos meses después de la baja del trabajador. También es habitual el uso abusivo de recursos informáticos, especialmente el acceso a Internet[44]. Los hechos pueden realizar el tipo penal del artículo 264 CP (*delito de daños*).

(3) *Información confidencial y datos personales*

Consiste en el acceso no autorizado y posterior revelación a terceros, generalmente competidores o clientes, de información confidencial de la empresa. En algunas ocasiones, la revelación la realizan trabajadores que tienen un acceso legítimo a la información pero sobre los que pesa una *obligación de reserva*. En este capítulo también se contempla la cesión no autorizada a terceros

[44] Aunque el uso abusivo no es *prima facie* un comportamiento delictivo, *vid.* SNIDER, L., *Crimes against capital: Discovering theft of time*, Social Justice, vol. 28, no. 3, 2001, pp. 105–120.

de datos personales de trabajadores y clientes. Los hechos pueden tener relevancia penal a la luz del artículo 197, 199 y 278 CP (*descubrimiento y revelación de secretos de personas físicas o de valor empresarial*), dependiendo del bien jurídico lesionado, en función de que la información afecte a la intimidad personal o a un secreto de empresa, y de si se el acceso a la información deriva del hecho de ser el responsable del fichero o de cualquier otra fuente de información.

(4) *Amenazas, injurias y calumnias*

El medio utilizado habitualmente es el correo electrónico corporativo, aunque también se han utilizado cuentas anónimas, e incluso se ha suplantado la identidad de otro trabajador de la misma empresa. En el caso de las amenazas, se busca un beneficio material o inmaterial para el trabajador. Si el beneficio no se produce, el trabajador llevará a cabo la conducta anunciada en el mensaje amenazador. En el caso de las injurias y las calumnias, se busca desacreditar a la empresa, o a alguno de sus directivos. También se han producido insultos a clientes habituales o a clientes potenciales de la empresa con los que el trabajador tenía algún conflicto[45].

[45] Las amenazas están tipificadas como delito en el artículo 169 y siguientes del CP, las injurias en el artículo 205 y siguientes del CP, y las calumnias están tipificadas como delito en el artículo 208 y siguientes del CP.

El informe señala tres clases más de infracciones habituales: infracciones relativas a la propiedad intelectual e introducción de obras de la empresa en redes P2P; intercambios de obras de terceros a través de redes P2P; e infracciones relativas a derechos de propiedad industrial.

V. Consideraciones finales

Internet, por la propia naturaleza del tipo de relaciones que conlleva, ha supuesto un incremento de oportunidades delictivas. Del análisis de los efectos criminógenos que están asociados al nacimiento de la red, se debería poder concluir que resulta conveniente, en términos de prevención de la delincuencia, tratar de corregir (i) la ausencia de controles externos eficaces; y (ii) una configuración de las reglas de navegación excesivamente generosa, que fomente un anonimato ilimitado y contraproducente.

La reducción de la esfera de privacidad que conlleva la adopción de un discurso de esta naturaleza no debería ser incompatible con dotar de las debidas garantías a los usuarios. Se deben buscar soluciones técnicas y jurídicas que permitan una utilización del espacio virtual que combine el necesario orden y control de las autoridades (seguridad) y la libre navegación de los usuarios (libertad).

En el contexto dialéctico entre libertad *versus* seguridad, la búsqueda de un punto de equilibrio no dejará de estar condicionada, en gran medida, por las opciones valorativas y políticas que sean dominantes en cada sociedad, sin perjuicio de que, en esta materia, más que en ninguna otra, sea necesario armonizar las reglas del juego, entre otras razones, por tratarse de un espacio inevitablemente globalizado.

VI. Referencias bibliográficas

Agustina Sanllehí, J.R. (2009), *Límites en las estrategias de prevención del delito en la empresa. A propósito del control del correo electrónico del trabajador como posible violación de la intimidad*, InDret 2/2009.

Agustina Sanllehí, J.R. (2009), *Privacidad del trabajador versus deberes de prevención del delito en la empresa. Cómo lograr el necesario equilibrio en las colisiones de deberes ante las nuevas herramientas de control empresarial,* Edisofer, Madrid.

Becker, G. (1968), *Crime and punishment: an economic approach*, Journal of Political Economy, 76.

Barnes, P., Lambell, J. (2002), *Organisational Susceptability to Fraud: Does Fraud Strike Randomly or Are There Organisational Factors Affecting its Likelihood and Size?*, Working Paper, Nottingham Business School.

Blount, E.C. (2003), *Occupational Crime. Deterrence, Investigation, and Reporting in Compliance with Federal Guidelines*, Florida.

Bryce–Rosen, C. (2007), «Youth Internet Victimization», *Current Issues in Victimology Research*, Moriarty & Jerin, 2nd edition, North Carolina.

Bussmann, K.–D. (2003), *Causes of Economic Crime and the Impact of Values*. *Causes of Economic Crime and the Impact of Values: Business Ethics as a Crime Prevention Measure*, paper presented at the Swiss Conference on Coping with Economic Crime. Risks and Strategies, Zurich.

Bussmann, K.–D., Werle, M.M. (2006), *Addressing Crime in Companies. First Findings from a Global Survey of Economic Crime*, British Journal of Criminology.

Davis, P., Francis, P., Jupp, V. (1999), *Crime–Work Connections: Exploring the 'Invisibility' of Workplace Crime*, in Davis, P., Francis, P., Jupp, V., Invisible Crimes. Their Victims and their Regulation.

Dickens, W.T., Katz, L.F., Lang, K., Summers, L.H. (1989), *Employee crime and the monitoring puzzle*, Journal of Labour Economics, 7.

Dodd N.J. (2004), *'Troublemaker' and 'Nothing to Lose' Employee Offenders Identified from a Corporate Crime Data Sample*, Crime Prevention and Community Safety: An International Journal 2004, 6 (3).

Kelling, G.L., Coles, C.M. (1996) *Fixing Broken Windows*: *Restoring Order and Reducing Crime in Our Communities*, New York, Touchstone Books.

McLaughlin, E., Muncie, J. (reprinted 2007), *The Sage Dictionary of Criminology*, Sage Publications.

Katyal, N.K. (2002), *Digital Architecture as Crime Control*, 111 Yale Law Journal 1039.
Felson, M., «Technology, Business and Crime», in Felson, M., Clarke, R.V. (ed.) (1997), *Business and Crime Prevention*, New York, pp. 81–96.
Ogburn, W.F. (1964), *On Culture and Social Change: Selected Papers*.
Gilfillan, S.C. (1935), *The Sociological Invention*, Cambridge, 1970 [originally published in 1935].
Kuhn, T.S. (1970), *The Structure of Scientific Revolutions*, (2nd ed), Chicago.
Weber, M. (1922), *Wirtschaft und Gesellschaft*, Tubingen, 1922 [translation as *Bureaucracy*, New York, 1946].
Hawley, A. (1950), Human Ecology: A Theory of Community Structure, New York.
Castells, M. (2003), *La Galaxia Internet*, Barcelona.
Eck, J.E. (1997) «Do premises liability suits promote business crime prevention?» in Felson, M., Clarke, R.V. (ed.), *Business and Crime Prevention*, New York, pp. 125–150.
Ribas Alejandro, J. (2003) *Aspectos Jurídicos del Comercio Electrónico en Internet*.
Jacobs, J. (1961) *The Death and Life of Great American Cities*, Harmondsworth: Penguin.
Newburn, T. (2007), *Criminology*, Portland, Oregon.
Newman, O. (1972) *Defensible Space: People and Design in the Violent City*. London, Architectural Press.
Thomas, D., Loader, B. (2000) *Cybercrime: Law enforcement, security and surveillance in the information age*, London: Routledge.
Rickman, N., Witt, R. (2007), *The Determinants of Employee Crime in the UK*, Economica.
Snider, L. (2001), *Crimes against capital: Discovering theft of time*, Social Justice, vol. 28, no. 3, pp. 105–120.