InDret

REVISTA PARA EL ANÁLISIS DEL DERECHO

WWW. INDRET.COM

El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio

Recensión a MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid, 2012, 332 páginas.

Constanza di Piero

Universidad de Navarra

BARCELONA, JULIO DE 2013

Ha acertado el autor en citar a Jorge Luis Borges. Los fragmentos transcritos de *Tlön, Uqbar, Orbis Tertius*; *La Biblioteca de Babel* y *El Aleph* dibujan con claridad lo que el lector encontrará al adentrarse en el texto: la descripción de un mundo distinto, cambiante y en constante progreso, pero también rápidamente obsoleto. Un mundo donde las interacciones se generan y se desarrollan de manera diferente a como lo hacen en el espacio físico y material. En definitiva, un mundo extraño al de los sentidos. El autor no sólo disecciona desde una perspectiva jurídico criminológica cómo opera el crimen en este nuevo lugar, sino que -motivado por una finalidad cognitiva y preventiva- también propone una categorización sistemática de la cibercriminalidad. Precisamente, en la introducción de la obra, remarca lo novedoso e incomprendido que resulta para la sociedad en general la relación que existe entre el fenómeno de la criminalidad y las Tecnologías de la Información y la Comunicación (TIC), y pone el acento en que este desconocimiento opera del mismo modo en las instituciones encargadas de su prevención. La nueva monografía que presenta el autor, nacida en realidad como «proyecto de artículo doctrinal» (p. 17), aborda el amplio y arduo tema del fenómeno denominado cibercrimen, extendiendo, así, su ya abundante investigación sobre la relación causal entre nuevas conformaciones sociales, surgimiento de nuevos intereses y necesidad de protección jurídica.

Las TIC han cambiado la forma de interrelacionarnos, y particularmente Internet ha modificado no sólo las relaciones económicas, sino también las políticas, sociales y personales, modificando el crimen como «evento social» y originando una nueva criminalidad. Los cambios experimentados como consecuencia de la utilización de herramientas tecnológicas no sólo hicieron surgir nuevas formas de afectar los intereses sociales, sino también afectaron a los protagonistas del fenómeno criminal: el autor y la víctima. El *hacker*, conocido como un personaje individual y solitario evoluciona y adquiere el papel de mafia organizada de cibercriminales, y otro tanto ocurre con la víctima del delito cibernético. No sólo cualquier persona física, jurídica o institución que se relacione en Internet puede ser víctima de un ciberdelito, sino también sus conductas cotidianas en este nuevo espacio pueden traducirse en plasmación de verdaderas políticas preventivas.

Con base en este análisis, el autor estructura la obra en dos partes. La primera parte, «Fenomenología del Cibercrimen», se compone de dos capítulos: «La criminalidad en el ciberespacio: la cibercriminalidad» y «Tipos de cibercrimen y clasificación de los mismos». Y la segunda parte, «Criminología del Cibercrimen», se divide en tres capítulos: «Ciberespacio y oportunidad delictiva», «El cibercriminal. Perfiles de delincuentes en el ciberespacio» y «La cibervíctima: perfiles de victimización y riesgo real de la amenaza del cibercrimen».

Para entender la obra es necesario conocer determinados conceptos. Precisamente por este motivo, en el primer capítulo, el autor delimita con notoria nitidez el alcance concreto de los términos cibercrimen y cibercriminalidad, sus posibles usos tipológicos y normativos, y la relación que existe entre ambos (p. 39). Subraya, siempre desde una perspectiva criminológica,

la necesaria sustitución del vocablo «delitos informáticos» por los de cibercrimen y cibercriminalidad, al no centrarse el riesgo en la «utilización de tecnologías informáticas» o en la «información del sistema informático», sino en el sistema de redes telemáticas intercomunicadas, y en las interrelaciones que allí se configuran (pp. 37 y 38). Se decide por un concepto amplio de cibercriminalidad: comprensivo de todas aquellas conductas (cibercrimen) en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión (ciberespacio) (p. 44).

En el segundo capítulo, el autor clasifica las diferentes tipologías de comportamientos criminales que existen en el ciberespacio con el objeto de comprender mejor su realidad criminológica. Sistematiza los cibercrimenes en dos grandes grupos (p. 50). El primero está conformado, según sea la incidencia que tengan las TIC sobre los comportamientos criminales, (i) ciberataques puros –comportamientos únicamente ciberdelictivos, ya que no sería posible su realización sin la existencia de las TIC- (p. 53); (ii) ciberataques réplica –comportamientos que ya existían en el mundo físico, pero su comisión en el ciberespacio los modifica-(p. 68); y (iii) ciberataques de contenido –que si bien entrarían dentro de los ciberataques réplica, presentan una problemática que un tratamiento privativo, que englobaría a todos los comportamientos cuyo núcleo delictivo es la transmisión de información a través del uso de las TIC- (p. 100). El segundo grupo de cibercrimenes responde a un criterio estrictamente criminológico, ya que tiene en cuenta el interés social afectado. Fracciona este grupo en tres grandes categorías: cibercriminalidad económica, social y política (p. 116). Si bien resalta el predominio cuantitativo de la cibercriminalidad económica, advierte sobre el progresivo protagonismo, tanto cuantitativo como cualitativo, de los cibercrimenes sociales, ya que al extenderse las interacciones sociales al ciberespacio, reducidas antes en el mundo físico, se multiplican las posibilidades de conductas delictivas (p. 122). Es esta última categorización (económica, social y política) la que el autor utilizará a lo largo de toda la obra para explicar las modificaciones que el ciberespacio ha provocado en los diferentes elementos del delito.

El tercer capítulo puede entenderse como el *anima* de la investigación. En él, MIRÓ LLINARES analiza la particular «arquitectura del ciberespacio» (p. 145), que conformada por elementos intrínsecos (tiempo/espacio) y extrínsecos (transnacionalidad, neutralidad, descentralización/distribución, universalidad, percepción de anonimización y evolución tecnológica) afecta, en definitiva, a la configuración del delito, lo cual alcanza a su comprensión y a su prevención. Realiza un análisis pormenorizado de las características de cada uno de éstos elementos y de las consecuencias que provocan en la configuración del delito, y sostiene que, a pesar de los efectos que las nuevas variables producen en el evento criminal, éste sigue siendo un delito que puede, y debe, ser explicado a través de las teorías criminológicas. Haciendo uso de la Teoría de las Actividades Cotidianas (TAC) de Cohen y Felson (p. 163), describe y analiza la manera en que el cibercrimen, presentado ya como un nuevo ámbito de oportunidad criminal, transforma cada uno de los elementos triangulares del

evento criminal: agresor motivado, objeto o víctima adecuada y ausencia de guardián capaz. Para la elección de la TAC, priman razones cognitivas, preventivas y legítimas (pp. 164-167).

Después de describir y explicar los caracteres del nuevo ámbito donde se desarrolla el cibercrimen, el autor analiza los efectos que el ciberespacio produce sobre la figura del agresor. Así, en el cuarto capítulo centra su estudio sobre los posibles perfiles criminológicos de los sujetos activos. De entrada, advierte sobre la imposibilidad fáctica de realizar un único perfil, y lo atribuye no sólo a la íntima relación que comparte el ciberagresor con el ciberdelito, sino también a la dificultad que presenta su persecución judicial. Por otro lado, hace notar que la ausencia de estudios criminológicos, cuantitativos y cualitativos, sobre perfiles concretos no permite brindar una conclusión general (p. 230). Es interesante, la presentación que hace «a modo de bestiario» (p. 231) de las diferentes características que concurren en los diferentes cibercriminales conforme a la descripción criminológica que realiza en el Capítulo II, resaltando las diferencias con el delincuente que opera en el mundo físico. Por ejemplo, en el caso del cibercriminal económico (p. 237), el perfil no responde a un sujeto concreto e individual, sino a una organización criminal, siendo el paradigma de esta ciberdelincuencia el *hacker*, sobre el que explica la transformación que ha sufrido. En la cibercriminalidad política (p. 250), resalta la diferente organización que presenta en relación con los agentes delictivos del mundo físico, y advierte sobre su organización horizontal y no vertical, con un objetivo central, al que se unen múltiples personas que comparten ideologías, sin necesidad de alto conocimiento técnico, y por tanto, prescindibles. Igualmente, no descarta la posible actuación individual, fuera de toda relación organizativa. Y por último, la cibercriminalidad social (p. 253): a la que presenta como la más compleja, especialmente, por la existencia de múltiples motivaciones en el sujeto activo, pero siempre con la particularidad que le impregna el ciberespacio. Analiza, por motivos fenomenológicos (p. 254), sólo tres perfiles: el *cybergroomer*, *cyberstalker* y el *cyberbuller*.

Finalmente, en el quinto capítulo, MIRÓ LLINARES centra su estudio en la figura de la víctima de la cibercriminalidad. Nuevamente, y al igual que en el capítulo anterior, subraya la imposibilidad de realizar un perfil único de esta figura (p. 261), por cuanto, en este ámbito de oportunidad delictiva (ciberespacio) el riesgo se configura no sólo por la motivación del sujeto activo, sino también, y muy especialmente, por la conducta que lleve a cabo cotidianamente la víctima (p. 263). A lo largo del capítulo, se empeña en resaltar la especial vulnerabilidad en que se encuentra la víctima virtual en relación con la víctima física, donde demuestra que no sólo pueden afectarse intereses patrimoniales, sino también personales. Pone el acento, además, en el efecto democratizador que ofrece Internet, y la relevancia de la conducta de la víctima. De nuevo, bajo el prisma de la TAC (p. 163), y la categorización criminológica propuesta (p. 50), el autor pone de relieve la vital importancia que adquiere en el ciberespacio la relación entre sus elementos configuradores, las conductas peligrosas que realiza la víctima, el tiempo que permanece ésta en el ciberespacio y la ausencia de guardianes capaces (barreras de protección) suficientes e idóneos (ya que muchas veces dependen de la propia víctima) para determinar conductas predictoras de su posible victimización (p. 267). El autor español, culmina la obra

ponderando la real dimensión del fenómeno de la cibercriminalidad (p. 292), y reflexionando sobre las posibles causas que están detrás de la falta de correspondencia cuantitativa entre los comportamientos cibercriminales y la posterior intervención judicial (p. 294).

En los párrafos precedentes, se ha intentado reflejar las principales ideas desarrolladas y sostenidas por MIRÓ LLINARES en su nuevo trabajo de investigación. Ahora bien, en los párrafos que siguen se pretende comentar, muy brevemente, ciertas reflexiones que la obra ha suscitado en la que suscribe.

Por de pronto, al finalizar la obra se comprende y se comparte la decisión tomada por el autor de aplazar el análisis dogmático de los delitos informáticos, y adentrarse al desarrollo del fenómeno del cibercrimen desde una perspectiva criminológica (p. 17). Dar cabida a un análisis jurídico, sin el trabajo previo de investigación que ha realizado MIRÓ LLINARES, adolecería de rigor científico; no sólo no se comprenderían las posibles dificultades jurídicas que la sociedad de la tecnología plantea, sino que tampoco podrían trazarse propuestas dogmáticas y soluciones políticocriminales acordes con los problemas. Precisamente, es lo que ha ocurrido, por ejemplo, con la tipificación del *online grooming* introducido por el legislador en la reforma operada por LO 5/2010, de 22 de junio. Se ha intentado dar una respuesta políticocriminal con notorio desconocimiento criminológico de los elementos configuradores, tanto del ámbito en el que se desarrolla el delito, como el de sus autores. Se resalta esta cuestión, por un lado, por la criminalización que ha sufrido el *grooming virtual*, y por el otro, por la relevancia dogmática y políticocriminal que poseen los delitos sexuales cometidos contra menores de edad. El legislador criminaliza, en aras de la importancia y de la efectiva protección del bien jurídico, determinados comportamientos que se encuentran situados en un estadio anterior de la concreta lesión del bien jurídico, e incluso posterior, como es el caso de la tenencia de pornografía infantil. Y paralelamente, la doctrina se encuentra compelida a ahondar en la laboriosa necesidad de legitimar esas conductas.

Según expone MIRÓ LLINARES (pp. 98 y 99), no todos los medios tecnológicos a través de los cuales se realiza el *cybergrooming* tienen la misma incidencia para la futura victimización, como tampoco ni los *groomers online* y *offline*, ni sus víctimas comparten el mismo perfil criminológico (pp. 255 y 288), y estas diferencias han llevado a los investigadores a concluir que el *cybergrooming* no comporta un mayor riesgo cualitativo que el *grooming* del mundo físico (p. 288). Sin embargo, pareciera como se ha dicho *ut supra*, que estos datos no fueron tenidos en cuenta para la tipificación del *child grooming*, ya que sólo se tipifica el que se realiza a través de las TIC y sobre un sujeto menor de 13 años. Y por otro lado, la redacción del tipo del 183 bis CP también permite la criminalización de conductas de ciberacoso. Esto hace indispensable mantener desde la doctrina la distinción de la diferente naturaleza de ambos comportamientos, y no referirse al ciberacoso como sinónimo de *grooming* (pp. 96, 287 y 306). La utilización indistinta de ambos términos, no favorece ni la comprensión ni la identificación de comportamientos *grooming*. No permite realizar estudios empíricos respecto de los perfiles criminológicos de los diferentes sujetos, como tampoco colabora en su correcto tratamiento jurídico penal, y en definitiva, en su prevención.

Ahora bien, puede que se pretenda sostener, o bien (i) que la comisión de estas conductas en el ciberespacio modifica las características esenciales del comportamiento (p. 99) obligando a transpolar el término «*on-line grooming*» a todo contacto que se realice a través de las TIC con la finalidad de abusar, agredir, acosar, explotar o corromper sexualmente al menor; o bien (ii) que por las dificultades del ciberespacio para la posterior persecución judicial de los comportamientos delictivos (p. 292) resultara necesario extender el alcance terminológico del término. En el primero de los supuestos, parece entonces más apropiado buscar un nuevo concepto integral y comprensivo de la mayor parte de los diferentes comportamientos «manipuladores» o «facilitadores» que se realicen a través de las TIC para introducir a menores en conductas sexuales, que revista independencia respecto de la tipificación realizada por el legislador, y que no se limite a abrazar sólo las conductas mayormente difundidas. La falta de idoneidad del término para reflejar su verdadera capacidad lesiva, ya fue advertida por la literatura al proponer reemplazar el término «*grooming*» por el de «*entrapment*» (GALLAGHER, 1998). En cambio, el segundo supuesto no supone modificaciones en la génesis del comportamiento, sino que la escasa actividad judicial demostraría que las reglas estructurales, es decir, institucionalizadas, en realidad están orientadas a mantener el orden dentro de un sistema social real. Si se considera el ciberespacio como un sistema (BRENNAN, 2004), el interrogante que se vislumbra, y que se echa en falta que el autor sólo lo mencione tangencialmente al responderse sobre la desproporción entre la actividad judicial y la comisión de cibercrimenes (p. 295), es si las normas y reglas en las que se asienta la actividad procesal del mundo físico deben, y hasta qué punto pueden, mantenerse vigente en el nuevo ámbito de oportunidad delictiva.

En este último sentido señalado, por ejemplo, el autor destaca, desde una perspectiva criminológica, el rol protagónico que adquiere la víctima en el ciberespacio, y que su actuación determina la configuración del riesgo criminal (p. 263). En concreto, señala que es el propio actuar de la víctima el que la convierte en un objetivo adecuado y no la voluntad del cibercriminal (p. 191). Por tanto, no se está ante una conducta neutral; en el sentido que no genera consecuencias, sino por el contrario, su comportamiento influye en la estructura, en la dinámica y en la prevención del delito. En este aspecto, los ciberdelitos podrían asemejarse, en parte, a los delitos de relación: delitos, en los que la víctima interviene y su comportamiento contribuye al hecho delictivo, y en mayor o menor medida, a la lesión del bien jurídico, disminuyendo o incluso eximiendo la responsabilidad del autor. Pero, rápidamente, se advierte la imposibilidad fáctica de aplicar *stricto sensu* esta regla, ya que se obligaría a la sociedad a cargar con el costo de asumir comportamientos imprudentes o inclusos dolosos de la víctima, precisamente porque al decir del autor es la única que en la práctica puede incorporar guardianes capaces para su autoprotección (p. 192). Con otras palabras, con qué validez, y en su caso, en qué proporción puede exigirse en el mundo virtual que la víctima adopte medidas mínimas de resguardo, como se exige, por ejemplo, en el delito de estafa. O, por el contrario debiera establecerse la regla que para los ciberdelitos rige el principio de autorresponsabilidad de la víctima, y que ésta cargue con la obligación de adoptar medidas de protección eficaces y efectivas, limitando la intervención del Derecho penal sólo a supuestos en

que no es posible la autoprotección. Al mismo tiempo, si la víctima se convierte en «[i]gnorante partícipe de ataques de todo tipo a otros usuarios» (p. 262), pareciera que tampoco son de utilidad las reglas actuales para la determinación de responsabilidad para el supuesto de complicidad, al no funcionar en el ciberespacio el *background* de experiencia adquirida para delimitar el ámbito de riesgo.

En suma, lo que se pretende, y que seguramente el autor tratará estas cuestiones en su próximo trabajo, es resaltar sucintamente que la divergencia existente entre la comisión de ciberdelitos y la posterior actividad jurisdiccional pueda también deberse a la dificultad que presenta el ciberespacio para orientar la conducta conforme a reglas constitutivas y prescriptivas que fueron creadas para ordenar y mantener las estructuras del mundo físico. Para continuar con la metáfora de Grabosky «*old wines in new bottles*» (p. 144), puede que la «arquitectura del ciberespacio» (p. 145) no permita utilizar viejos odres para contener el nuevo vino (Lucas 5:37), ya que el nuevo vino necesita de nuevos odres, porque los viejos ya no sirven para contenerlo, y el nuevo vino se derrama y se derrocha. Es cierto que el ciberdelito es delito (p. 145), pero también es cierto que es ciber, y si se pretende encorsetar el sistema del ciberespacio en el orden social real, puede que debamos renunciar o reformular ciertas reglas.

Por otra parte, es muy destacable el agrupamiento sistemático propuesto, superador de tipos penales concretos, y con capacidad de alcance universal. Además, está provisto de gran valor didáctico, por cuanto ordena y clasifica los múltiples comportamientos ciberdelictivos, y favorece el tratamiento conjunto de diferentes aspectos. El conocimiento del autor se aprecia en el volumen de la bibliografía que maneja, tanto nacional como extranjera, concretamente del mundo angloamericano. Se agradece también el empleo de gráficos; aportan mayor claridad al contenido de su exposición, como también la incorporación del glosario en la parte final de su obra. Del mismo modo, debe resaltarse la cuidada redacción a lo largo de todo el trabajo. Puede afirmarse que la obra de MIRÓ LLINARES será referente obligado para todo aquél que pretenda conocer y comprender el fenómeno del cibercrimen, y también para pensar y trazar políticas preventivas reales. Se espera con impaciencia la segunda obra prometida.