Estudios Penales y Criminológicos, vol. XLI (2021). https://doi.org/10.15304/epc.41.6718
ISSN 1137-7550: 705-777

NUEVOS RETOS DOGMÁTICOS ANTE LA CIBERCRIMINALIDAD
¿ES NECESARIA UNA DOGMÁTICA DEL CIBERDELITO ANTE UN NUEVO PARADIGMA?

José R. Agustina*

Resumen: En el presente trabajo se cuestiona si es o no necesario emplear un enfoque distintivo y adaptar algunas categorías dogmáticas de la teoría del delito ante los retos que plantean los delitos cometidos (en su integridad o de forma preponderante) en el ciberespacio. Para ello, se parte de una comprensión amplia de la naturaleza y dimensión de los cambios experimentados en la era digital y se propone una definición funcional del concepto de ciberdelito para las distintas perspectivas de análisis: criminológica, penal, procesal y dogmática. La tesis principal es que el contexto y fenomenología virtual exigen una relectura transversal de los contornos que delimitan algunas categorías dogmáticas. El motivo no obedece a

Recibido: enero 2021. Aceptado: mayo 2021

* Catedrático de Derecho Penal. ORCID: 0000-0002-9254-6902
Universitat Abat Oliba CEU. Dirección: Bellesguard, 30
08022, Barcelona. Email: jagustinas@uao.es

una nueva expansión del Derecho penal, sino a un cambio de paradigma de naturaleza antropológica y sociológica sin precedentes: el ser humano y sus operaciones esenciales como agente (conocer y querer), la propia fenomenología de la acción humana y sus efectos en el mundo "exterior" (offline y online) se han visto alterados o, cuando menos, condicionados ante un contexto tecnológico que, por sus efectos disruptivos, debería tener reflejo en la arquitectura dogmática. Se presentan de forma programática algunas cuestiones y se analiza la repercusión del cambio de paradigma en algunas categorías del sistema, en particular, en los conceptos de acción y bien jurídico.
Palabras clave: ciberdelito y teoría del delito; nueva dogmática; concepto de acción; bien jurídico; relación criminología y derecho penal.

NEW CHALLENGES FOR CRIMINAL LAW THEORY BEFORE CYBERCRIME

Is it necessary to build a new Criminal Law Theory for cybercrime due to a new paradigm?

Summary: In this article the author questions if it is necessary to use a distinctive focus and adjust some doctrinal categories within the Criminal Law Theory before the new challenges risen by crimes committed in cyberspace. For this aim, he parts from a wide comprehension of the nature and dimensions due to the changes derived from the digital era and proposes a functional definition of cybercrime for any type of analysis –criminological, legal, procedural or doctrinal. The main point developed in this paper is that the virtual context and phenomenology require a transversal understanding of the boundaries which define some doctrinal categories. The reason is not due to a new expansion of Criminal Law, but to an unprecedented anthropological and sociological paradigm shift: the human being and its essential operations as an agent (knowing and willing), the phenomenology of human action and its effects on the "outside" world (offline and online) have been altered or, at least, conditioned by a technological context that, due to its disruptive effects, should be reflected in the Criminal Law Theory architecture.

Some issues are presented programmatically and the impact of the paradigm shift in some categories of the system is analyzed, particularly in the concepts of action and legal good.
Keywords: cybercrime and Criminal Law Theory; new approaches to Criminal Law Theory; concept of action; legal good; Criminology and Criminal Law relationship.

Sumario. 1. Introducción: tres premisas erróneas. 2. De lo exterior a lo interior: dimensiones y alcance del cambio de paradigma. 3. Bases para una teoría del delito adaptada a la era digital. 4. Sobre el concepto de ciberdelito y su función en el marco de la teoría dogmática. 5. Hacia una propuesta de revisión de algunas categorías, subconceptos o estructuras de imputación de una teoría del delito adaptada a la era digital. 5.1. Modulaciones en el concepto de acción y sus implicaciones dogmáticas. 5.2. Modulaciones en el concepto de bien jurídico. 5.3. Imputación objetiva, autoría y participación y otras cuestiones. 6. Conclusiones. 7. Bibliografía.

Strumming my pain with his fingers
Singing my life with his words
Killing me softly with his song[1]

1. Introducción: tres premisas erróneas[2]

En anteriores trabajos, me había aproximado al análisis del ciberespacio como lugar particularmente propicio

1 Fragmento de la letra de la canción "Killing Me Softly with His Song", escrita por Norman Gimbel en colaboración con Lori Lieberman que en 1973 se popularizó en la versión cantada por la artista Roberta Flack.

2 Este trabajo ha sido realizado en el marco del Proyecto "Criminología, evidencias empíricas y política criminal" (Ref. DER2017-86204-R), financiado por el Ministerio de Ciencia, Innovación y Universidades, y empezó a redactarse con motivo del seminario impartido en la Universidad Externado de Colombia inicialmente previsto en noviembre de 2019. Desearía hacer constar mi agradecimiento a Ricardo Posada,

para la generación o atracción de comportamientos delictivos[3]. Con posterioridad, me centré en el problema de los ciberdelitos desde una perspectiva victimológica (con alguna muy leve incursión en el terreno victimodogmático), con el fin de *explicar para prevenir* las conductas ingenuas por parte de la víctima que, por las características propias del entorno, facilitan la perpetración de ciberdelitos[4]. Ese enfoque, sin duda, abría el análisis sobre un fenómeno nuevo, complejo y en expansión, exigiendo aportes de distintas disciplinas, como la criminología, la psicología, la antropología e incluso la educación[5]. Sin embargo, en el ámbito propiamente

---

Fernando Miró, Laura Mayer, Javier Cigüela y Marcos Salt por la lectura previa del texto y sus valiosos comentarios y sugerencias.

3 Véase, AGUSTINA, «La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual», *International E-Journal of Criminal Sciences*, 2009, 3, pp. 1-31, en donde utilizo la dicotomía entre lugares que generan (*crime–generators*) o atraen delincuencia (*crime–attractors*) empleada por Eck (1997). Véase también, KATYAL (2002), *Digital architecture as crime control*. Yale Law Journal, 112, 2261. Sobre el ciberespacio como nuevo espacio de oportunidad delictiva, Miró, «La oportunidad criminal en el ciberespacio», *Revista Electrónica de Ciencia Penal y Criminología*, 13-07, 2011, pp. 1-55.

4 Véase, AGUSTINA, «Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización», *Cuadernos de Política Criminal*, 2014, 114(III), pp. 143-178, en donde, partiendo de la metáfora de que *Internet es un lugar oscuro* en el que convendría arrojar algo más de luz y poner cierto orden, se sugiere observar cierto paralelismo y trasladar al ciberespacio la lógica de la prevención aplicada al mundo físico. *Mutatis mutandis*, habría que trasladar al mundo virtual el deseo sentido de que las calles y barrios de nuestras ciudades sean un lugar seguro. Ese deseo se ha traducido en todo un conjunto de medidas: desde el diseño arquitectónico del espacio público, el patrullaje policial o la creación de lazos comunitarios entre el vecindario, hasta las propias cautelas de los viandantes, que saben por qué lugares (y a qué horas) es mejor no transitar. Sin duda, en las interacciones en el ciberespacio la conciencia del riesgo por parte de la víctima y su propia conducta resulta decisiva.

5 Sobre los efectos multidisciplinares de la transformación del mundo físico y su traslación al ciberespacio, así como sobre las importantes mutaciones psicológicas, culturales, educativas y también victimológicas,

del Derecho penal, más allá de los acercamientos prácticos surgidos ante la necesidad imperiosa de regular las nuevas figuras de delito y obtener evidencias digitales, no existía apenas una reflexión teórica sobre una nueva tendencia que –los años lo han constatado así– había venido para quedarse. A este objetivo me dedicaré en el presente trabajo.

Probablemente, ha llegado la hora de *hacer de la necesidad virtud* o, al menos, de plantearse qué tiene que decir la dogmática penal sobre el ciberdelito en sus características estructurales y cómo influye el cambio de escenario en la reflexión teórica y en las categorías del sistema jurídico del delito. Para ello, trataré de ensamblar, no sin dificultades, las distintas perspectivas aplicadas a esta nueva realidad. El propósito es ambicioso y, por limitaciones de espacio, en estas líneas solo se apuntarán algunas ideas rectoras de una visión dogmática con pretensiones integradoras.

Tal vez *los árboles no nos han dejado ver el bosque*. La irrupción del cibercrimen solo ha provocado una primera respuesta a algo que parecía un problema no estructural. Sin embargo, poco a poco, esa respuesta debería permear todo el sistema. Como es sabido, a pesar de la importante cifra negra que, en los últimos años, enmascara la verdadera incidencia de la cibercriminalidad, es ya un lugar común referirse al reto que plantea como un desafío inaplazable[6]. Con frecuencia, los medios de comunicación han venido centrando en la criminalidad organizada la relevancia de este nuevo desafío. Sin embargo, con el avance de la investigación criminológica, se

véase, MONTIEL/AGUSTINA, «Retos educativos ante los riesgos emergentes en el ciberespacio», *Revista Española de Pedagogía*, 2019, 77(273), pp. 277-294.

6 Sobre la cifra negra relativa a la cibercriminalidad y sus causas, véase CANEPPELE/AEBI, «Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes», *Policing: A Journal of Policy and Practice*, 2019 13(1), 66-79; LAVORGNA, *Cybercrimes*, 2020, p. 18 y ss.

puede afirmar que la tecnología constituye un aliado y facilitador casi omnipresente (aunque sea de forma incidental) de la delincuencia más común. En efecto, en todos los delitos las TIC juegan actualmente un papel relevante, ya sea por algunos elementos del concreto *modus operandi* del delito, por la fase preparatoria (no necesariamente punible) o post-consumativa (amplificando los efectos del delito a través de la red), o por el rastro digital que a efectos probatorios lleva consigo.

La tecnología y el Derecho penal parecen, pues, estar llamados a entablar un diálogo fluido y entenderse a fondo si se pretende hacer frente al *efecto desplazamiento*[7] de una buena parte de las infracciones penales a ese nuevo lugar o espacio *sui generis*, donde el principio de territorialidad de la ley penal cada vez plantea más inconvenientes.

Pues bien, la falta de respuesta o interés de la dogmática (o su retraso)[8], a mi juicio, se debe a tres premisas erróneas que, de forma implícita, entorpecen la labor de conjunto que es necesaria ante un envite de tanta magnitud. *En primer lugar*, no se puede descartar de plano que la reflexión dogmática sea relevante simplemente porque *nos hallamos ante un problema de orden práctico*. Esa ha sido la prioridad: la respuesta de los Estados y la atención de la doctrina se han centrado en dar una respuesta jurídico-técnica al problema tratando de salir al paso de las posibles lagunas de punibilidad (perspectiva de Parte Especial) o de las dificultades en

7 CANEPPELE/AEBI, «Crime drop or police recording…; MIRÓ/MONEVA, «Environmental Criminology and Cybercrime: Shifting Focus from the Wine to the Bottles». *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 491-511.

8 De acuerdo con la teoría de Ogburn, los cambios tecnológicos son el motor de cambio en la cultura y en la sociedad, aunque con cierto retraso (*cultural lag*). Véase, OGBURN, *On culture and social change: selected papers*. Chicago: University of Chicago Press. Sobre el impacto de la teoría de Ogburn en la criminalidad, Felson, "Technology, Business and Crime". In Felson, M., Clarke, R.V. (eds.), *Business and Crime Prevention*, Criminal Justice Press, New York, 1997, pp. 81–96.

la obtención y práctica de prueba (perspectiva procesal) ante un escenario desconocido y que, de suyo, presenta una complejidad mucho mayor sobre todo si no se proporciona la formación adecuada a los operadores jurídicos.

Sin perjuicio de que se persiga una respuesta rápida y eficaz, la reflexión dogmática es siempre necesaria ante cualquier cambio social de cierta relevancia que, como es el caso, tenga implicaciones en la naturaleza del ser humano o en los valores y principios básicos de política criminal. A este respecto, pues, parece haberse asumido, en una *segunda premisa*, que la dogmática es una arquitectura inmutable ajena a una *moda esnobista* como el cibercrimen. Con muy pocas excepciones[9], la doctrina penal ha parecido no prestar atención, casi como si fuera algo veleidoso, a las repercusiones en el sistema del cambio sociológico más disruptivo, sin duda alguna, en la historia de la humanidad. El crecimiento exponencial de los cambios tecnológicos solo augura un mayor desfase, cada vez más vertiginoso, con el estadio anterior[10].

9 Sobre la necesidad en general, véase, POSADA MAYA, «El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual», *Nuevo Foro Penal*, 13(88). Algunos trabajos enfocados a problemas concretos empiezan a sugerir que, en efecto, se requiere una modulación en el análisis. Véase, por ejemplo, el excelente trabajo de COCA VILA, «Coches autopilotados en situac iones de necesidad: una aproximación desde la teoría de la justificación penal», *Cuadernos de Política Criminal*, núm. 122, II, Época II, septiembre 2017, pp. 235-275. En general, las reflexiones de la doctrina se han mantenido en el plano de la teoría de la interpretación, como un problema de mera tipicidad.

10 GOODMAN, *Los delitos del futuro*, Ariel, 2015, p. 62. Estamos acostumbrados a seguir un pensamiento lineal con respecto a los cambios y la tecnología sigue un proceso de aceleración distinto. Marc Goodman, utilizando la metáfora de las hojas de nenúfares que se duplican cada día en la superficie de un estanque, advierte de que nos hallamos cerca de llegar al día 29. El primer día se pasa de 1 a 2; el segundo, de 2 a 4; el tercero, de 4 a 8… La progresión va aumentando exponencialmente y llegados al día 27 se cubriría 1/4 del estanque; el día 28 saltaría a la mitad y el día 29 todo quedaría cubierto por nenúfares, impidiendo la pervivencia del ecosistema. Tales predicciones se apoyan en los postulados de la conocida ley de Moore, que establece un patrón de

Parece incomprensible el silencio de la dogmática, aunque tal vez se comprenda por la resistencia o simple pereza a enfrentarse a lo desconocido y tener que entenderse con ese *submundo* de la informática, con su lenguaje inaccesible al profano.

Ese inmovilismo o falta de respuesta debería cuestionarse. Como veremos, el concepto de acción, como premisa embrionaria de todo el sistema, no quedó anclado en el paradigma causal-positivista del s. XIX, ni en los aportes del finalismo. Siendo un hijo de su tiempo, ese concepto ha ido atravesando diferentes etapas, en una evolución que llega hasta las puertas de la era digital. ¿Acaso no debería reflexionarse al respecto? La teoría del delito es una estructura permeable y sensible al devenir socio-cultural de la sociedad. Siempre surgen cuestiones nuevas y los viejos problemas, con el tiempo, adquieren contornos distintos que, en ocasiones, exigen modulaciones no menores. La misión dirigida a la formación del sistema no termina nunca[11]. En ese sentido, para lograr una respuesta adecuada desde el Derecho penal, se hace preciso enmarcar el momento presente en los estadios de evolución de la teoría del delito, en las coordenadas históricas en las que nos encontramos.

El Derecho penal moderno tiende a explicarse como el efecto de la industrialización y de la Ilustración[12]. Tras la posmodernidad, la globalización y, ahora, la intensificación de la era digital, los parámetros de valoración de los conceptos

---

duplicación persistente en la capacidad de procesamiento. KURZWEIL (2005), siguiendo esa lógica no del todo demostrada, sitúa el año 2045 como punto de inflexión definitivo en la *singularidad*, advirtiendo que en los próximos años se vivirá "un cambio tecnológico tan acelerado y profundo que representará una ruptura en el tejido de la historia de la humanidad".

11 Por todos, JESCHECK/WEIGEND, *Tratado de Derecho Penal,* 2002, p. 213.

12 VORMBAUM, *Einführung in die moderne Strafrechtsgeschichte*, 2020, p. 18.

de delito y pena, así como del propio sistema, requieren ajustes importantes o, más bien, una reconceptualización. La sociedad de riesgos y la sociedad-red son, en este contexto, la antesala de un cambio de paradigma hacia algo más ecléctico, con efectos sinergéticos. El delito se ha virtualizado en una sociedad transparente[13] y es más que nunca comunicación de sentido en un escenario nuevo, con reglas distintas y con efectos inmediatos. El lenguaje del proceso penal y el lenguaje de la sociedad, como el lenguaje de la política criminal, deben converger en algún punto si el sistema no se concibe como una realidad autopoyética. Para todo ello, es esencial la teoría de medios[14] y entender que los "medios no sólo transmiten mensajes, sino que producen el efecto de moldear nuestro pensamiento, percepción, memoria y comunicación"[15]. Se debe comprender desde el sistema penal, también, que la tecnología está cambiando las reglas de la convivencia humana, llegando a afectar a los modelos de control social y la diferenciación entre medios normativos y cognitivos, así como el mismo concepto de libertad humana[16].

Mutatis mutandis, la doctrina penal sí salió al paso –con mayor o menor celeridad– de los cambios estructurales

13 Sobre el concepto de sociedad transparente, al que se hará referencia más adelante, véase HAN (2014).

14 VESTING, *Legal theory and the media of law*, Edward Elgar Publishing, 2018.

15 KRÄMER, *Medium, Bote, Übertragung - Kleine Metaphysik der Medialität*, 2008, p. 14; ONG, (nota al pie 4), p. 81 ["Technologies are not mere exterior aids but also interior transformations of consciousness"].

16 Sobre la transformación de las formas de control en una "sociedad de la transparencia", véase HAN (2014); sobre cómo ha evolucionado el ciberespacio e Internet, desde un espacio de anarquía a un espacio de control, donde el código es ley (*Code is Law*), véase LESSIG (2006), *Code 2.0*, Basic Books. Lessig señalaba de forma profética cómo cuando observamos el camino por el que evoluciona el ciberespacio (¡en 2006!), vemos que mucha de esa "libertad" que estaba presente en el momento de fundarse ese ciberespacio idealizado será removida en el futuro: nos arrepentiremos entonces de las decisiones tomadas y trataremos de desandar el camino (p. 5).

que supuso la expansión del Derecho penal a la delincuencia económica. A este respecto, sobre la relación entre el sistema y las categorías e instituciones que lo conforman, Silva Sánchez vino a señalar que el motor esencial del cambio evolutivo del sistema de la teoría del delito a lo largo de la historia ha sido la propia evolución cultural de la sociedad[17]. Ante la criminalidad económica fue necesario un ejercicio de adaptación a todos los niveles (legislativo, dogmático y jurisprudencial). Las causas de aquel giro político-criminal son complejas desde un punto de vista sociológico[18]. Y esa es la línea que planea sobre el presente texto: verificar si la tensión por aprehender los problemas nuevos debería forzar al sistema a reformular determinadas instituciones dogmáticas. El sistema debe siempre estar atento a los procesos de cambio y, por lo que aquí interesa, adaptarse a la era digital con todas sus consecuencias desde el punto de vista psicológico o antropológico, criminológico, cultural o económico[19]. Así, pues, ¿no debería analizarse si, en términos de garantías o imputación objetiva, habría que desgajar, como una porción o subparte del sistema, cuando menos algunas manifestaciones de la cibercriminalidad? ¿Nos encontramos ante un nuevo supuesto de Derecho penal *de tercera velocidad*?[20]

En tercer lugar, la resistencia a plantearse cualquier cambio estructural en el sistema se ha apoyado en que estamos ante *vino viejo* que nos hemos empeñado en poner *en odres nuevos*[21]. La tecnología puede cambiar rápidamente,

17 SILVA SÁNCHEZ, "Teoría del delito y Derecho penal económico-empresarial". En SILVA SÁNCHEZ/ MIRÓ LLINARES, *La teoría del delito en la práctica penal económica*. La Ley, Madrid, 2013, p. 33-34.

18 SILVA SÁNCHEZ, *La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, 2001, *passim*.

19 Véase, al respecto, AGUSTINA, "Cibercriminalidad y perspectiva...", p. 145 y ss.

20 SILVA SÁNCHEZ, *La expansión del derecho penal, passim.*

21 GRABOSKY, "Virtual criminality: Old wine in new bottles?", *Social & Legal Studies*, 10(2) 2001, 243-249, donde afirma: "a great deal of

pero la naturaleza humana, no. Desde ese punto de vista, solo han cambiado los medios. La novedad del cibercrimen residiría en la capacidad sin precedentes para poder cometer delitos movidos por las mismas motivaciones de siempre (con la codicia o ánimo de lucro como primer motor psicológico)[22]. Por tanto, según ese discurso, nada habría cambiado *en lo esencial*. A efectos jurídico-penales, por tanto, bastaría con examinar desde el punto de vista del principio de legalidad las posibles lagunas de punibilidad que, en ocasiones, podrían considerarse superfluas, pues los delitos, en su núcleo esencial, no han cambiado (*nihil novum sub sole*). A tenor de dicha lectura del nuevo escenario que irrumpe con la era digital, los problemas que plantean los discursos hiperbólicos en torno a los cambios dramáticos en las formas de criminalidad se resolverían en el nivel del juicio de subsunción y en la renovación de los adecuados instrumentos procesales, sin llegar más lejos.

2. De lo exterior a lo interior: dimensiones y alcance del cambio de paradigma

Aquí es donde se situaría el punto de arranque de estas líneas. En las dos últimas décadas, con el rápido avance de la transformación digital, el modo de relacionarnos los seres humanos y de causarnos daño ha experimentado mutaciones significativas, proporcionando una diversidad de medios y formas de ataque antes inimaginable. Ciertamente, a primera vista parece un simple cambio de contexto con importantes repercusiones. Debido a la hiperconexión digital, todo es mucho más fácil y rápido para el delito y, en ese

crime committed with or against computers differs only in terms of the medium. While the technology of implementation, and particularly its efficiency, may be without precedent, the crime is fundamentally familiar".

22 GRABOSKY, "Virtual criminality: Old wine in new bottles?", 2001, pp. 243-244.

sentido, cuanto más conectados estamos, somos más vulnerables[23]. Así, se puede intentar cometer un ciberfraude masivo a miles de kilómetros de distancia mediante una sola acción, pudiendo causar un impacto en miles de víctimas al mismo tiempo, cada una en una punta distinta del planeta. Se pueden lesionar bienes personales con una facilidad e inmediatez inusitadas: generando de forma instantánea una noticia falsa e injuriosa en una red social; contactando con fines sexuales con menores a los que (solo por lejanía física) hubiera sido imposible acceder hace tan solo unos años; o provocando, mediante la utilización abusiva de datos personales de la víctima, que cientos o miles de personas la contacten alterando, como mínimo, su tranquilidad emocional.

¿Tienen razón entonces cuando se afirma que lo que plantea el cibercrimen es una mera cuestión de medios, facilidad comisiva, rentabilidad o escalabilidad y de cómo resolver cuestiones prácticas en la persecución de tales infracciones en el ciberespacio?

En realidad, tales cambios no son periféricos, contextuales o meramente epidérmicos –ese es el nervio de mi discurso–. Ni son neutros al individuo que debe interaccionar en un nuevo espacio donde las percepciones y precomprensiones son distintas a las propias del mundo físico. En el ámbito de la cibercriminalidad, en primer lugar, el espacio se contrae y el tiempo se comprime[24]. Este factor por sí solo plantea ya interesantes cuestiones sobre la unidad de medida y los problemas de concurso de normas y/o de delitos, como se verá. Junto a ello, la bilocación o ubicuidad y el desdoblamiento de la persona en tiempo real pueden conllevar distintos problemas cognitivos o volitivos. Además, las interacciones más o menos automatizadas o programadas pueden desdibujar, en el sujeto activo, atributos esenciales de

23 GOODMAN, *Los delitos del futuro*, 2015, p. 11.

24 Por todos, MIRÓ, *El cibercrimen*, 2012.

la acción (por ejemplo, de engañar: ¿se puede engañar a una máquina?) o, en el sujeto pasivo, hacerle perder el dominio del hecho sobre la transmisión no consentida de activos o la causación de daños a terceros (al propagar un virus dentro de una organización). Todas estas cuestiones podrían verse no solo como un aparente problema de tipicidad.

Pero no todo se reduce a un cambio de contexto espacio-temporal. Los protagonistas interaccionan en un lugar oscuro con características propias, donde se promueve el anonimato, factor criminógeno de primer orden[25]. En esas calles oscuras de Internet, la apariencia de ofensor y víctima, cuando media la tecnología, puede ser un muy pálido reflejo de la realidad. La influencia del medio no solo afecta a esa apariencia superficial de los individuos, sino que acaban viéndose ellos mismos afectados. De lo exterior a lo interior y de lo accidental a lo esencial: más allá del cambio en el modo de presentarse y en las actividades cotidianas (con el notable incremento de las interacciones online y, por tanto, de las oportunidades delictivas[26]), el ser humano mismo ha visto moduladas algunas de sus facultades más esenciales. La tecnología, como anticipamos en líneas anteriores, nos transforma más allá de nuestros hábitos y costumbres, llegando a modular de forma inadvertida el modo de captar y conocer la realidad, manifestar afecto o voluntad hacia algo, estar presente aquí o allá… Como hipótesis, podría sostenerse que el ciberespacio en cuanto nuevo contexto existencial (1) ha

25 En su aplicación al ciberespacio, véase KATYAL, Digital architecture as crime control. *Yale Law Journal*, 112, 2002, 2261.

26 En general, sobre el impacto en las tasas del delito a consecuencia de los cambios en las actividades cotidianas y estilos de vida, véase, COHEN/FELSON, Social change and crime rate trends: A routine activity approach. *American sociological review*, 1979, 588-608; HINDELANG, GOTTFREDSON/GAROFALO, *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger, 1978. Sobre su incidencia en las interacciones mediadas por la tecnología, véase MIRÓ, «La oportunidad criminal en el ciberespacio», 2012, *passim*.

oscurecido la inteligencia humana y la forma de percibir la realidad en un mundo en el que lo real, frente a lo aparente, se ha banalizado y donde los niveles de engaño/error han proliferado hasta extremos preocupantes; (2) y ha debilitado la voluntad, agigantando tendencias impulsivas innatas o generando nuevas patologías que han llegado a normalizarse[27]. El ser humano, con su naturaleza herida, ha perdido capacidad de discernimiento y autocontrol[28], quedando sensiblemente condicionado[29]. En esta *nueva* versión del ser humano, más

27 Véase, AGUSTINA, «Cibercriminalidad y perspectiva victimológica…», p. 178, donde se refiere a la célebre disputa filosófica entre Heráclito y Parménides en la Antigua Grecia sobre la tesis del flujo universal de los seres –«panta rei» (πάντα ρεῖ): todo fluye–. En dicha discusión, ya se puso de manifiesto que, en realidad, aunque un hombre no puede bañarse dos veces en el mismo río (pues la segunda vez, el río ya no es el mismo, como tampoco lo es el hombre), no por ello el ser humano pierde sus atributos esenciales a pesar del fluir de los cambios. En efecto, en la naturaleza humana hay una parte esencial que resiste a los cambios históricos y culturales, y también tecnológicos, pese a que tales cambios pueden afectar enormemente las condiciones relacionales, los estilos de vida y, en lo que ahora interesaba, las categorías con que opera la teoría del delito.

28 La conducta delictiva surge, según la teoría general de Gottfredson y Hirschi, del bajo autocontrol de la persona o de su baja capacidad para contener su propio comportamiento a través de su regulación interna. La mayoría de los delitos consisten en acciones relativamente simples que proporcionan gratificaciones inmediatas, surgidas en un instante y realizadas sin dar importancia a las consecuencias que llevan aparejadas. Los sujetos que cometen la mayoría de delitos presentan características comportamentales y actitudinales comunes, incluyendo la impulsividad, falta de sensibilidad y poca consideración hacia el futuro (GOTTFREDSON/HIRSCHI, *A general theory of crime*. Stanford University Press, 1990). El autocontrol es uno de los factores predictivos que correlacionan con mayor consistencia con la comisión de hechos delictivos: véase, PRATT/CULLEN, The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis, *Criminology*, 38, 931-964. Sobre su incidencia en la cibercriminalidad y también en la victimización on line, véase, HOLT/BOSSLER/SEIGFRIED-SPELLAR, *Cybercrime and digital forensics: An introduction*. Routledge, 2015, pp. 290-293; 306-308.

29 Me apoyo aquí en el modelo antropológico esbozado por SILVA SÁNCHEZ, *Malum passionis. Mitigar el dolor del Derecho penal*, 2018,

superficial y emotiva, más voluble y vulnerable, la conducta humana penalmente relevante se ve en parte alterada[30].

Tales cambios empujan a pensar en que los criterios de atribución y el sentido de nuestras acciones requieren de una reconceptualización, pues ya en el inicio de toda acción mediada por la tecnología el grado de advertencia con que se toman decisiones *no es el mismo*. Como tampoco es el mismo el estado (corpóreo *versus* digital) de nuestros interlocutores, ni los efectos del delito. Lo físico, sin dejar de ser el punto de anclaje del individuo, se proyecta hacia una realidad virtual en expansión, con cada vez más apéndices o avatares bajo el propio control.

En otro lugar, nos hemos referido a una suerte de esquizofrenia digital o trastorno disociativo de la personalidad facilitado por las características del ciberespacio, en el que nada es lo que parece[31]. Sin embargo, ese desdoblamiento del

---

pp. 23-24, en donde se define al ser humano como "un sujeto con conocimiento limitado y voluntad imperfecta […]. Alguien necesitado de ayuda y condicionado, pero con un margen para la libertad".

30 Soy consciente de que la profundidad e implicaciones antropológicas y jurídicas de tales afirmaciones exceden un trabajo como el presente. Desarrollando la idea primigenia de Ortega y Gasset (1914), se puede sostener hoy, en cuanto a la identidad personal, que el yo soy yo y mis circunstancias está condicionado fuertemente por la aparición y posterior dependencia del *smartphone*. Y si al principio se celebró la red digital como un medio de libertad ilimitada, esa ilusión ha evolucionado hasta convertirse en control y vigilancia totales, siendo así que los residentes del panóptico digital se comunican intensamente y se desnudan por su propia voluntad (HAN, 2014). Sobre los efectos psicológicos y adictivos del *smartphone*, véase ALTER (2017), *Irresistible: The rise of addictive technology and the business of keeping us hooked*. Penguin; MONTIEL/AGUSTINA, Retos educativos…, *passim*.

31 Véase, AGUSTINA, «Cibercriminalidad y perspectiva victimológica…», p. 162, en relación al efecto desinhibidor que describe SULER, «The Online Disinhibition Effect», *Cyberpsychology & Behavior*, Volume 7, Number 3, 2004, en donde se interroga: "What elements of cyberspace lead to this weakening of the psychological barriers that block hidden feelings and needs?" (p. 322; AGUSTINA/MONTIEL/GÁMEZ, Cibercriminología y victimización online, 2020, pp. 30-34.

yo-real al yo-digital (o a los diversos *yoes*), ha evolucionado hacia una confusión de planos, en tanto que la constante intermitencia nos ha instalado en una realidad híbrida en la que se dificulta mucho separar con nitidez los mundos offline y online. Todo este giro antropológico tiene consecuencias en el lenguaje jurídico y en las categorías tradicionales; en la forma de definir los derechos fundamentales y las esferas jurídicas garantizadas; y, en lo que aquí interesa en última instancia, en la forma de imputar responsabilidad penal.

No es una pura metáfora afirmar que podemos *matar* a alguien con una canción (como decía Roberta Flack en la cita antepuesta: *"killing me softly with his song"*). Las palabras y las relaciones a través de avatares o máscaras en el ciberespacio pueden causar verdadero daño, aunque este se produzca en una "realidad simulada"[32]. Herir a través de conexiones virtuales es distinto, posee unas reglas y caracterización propias. Ya sabíamos que nuestra identidad era algo más que su dimensión corporal (adición al yo-real del yo-digital, en sus diversas formas). Sin embargo, ahora se tiende a la plena equiparación entre ambas realidades a efectos de ser sustrato del mismo bien jurídico, incluso en delitos de propia mano. Como botón de muestra de esa equivalencia valorativa plena, es ya doctrina consolidada del Tribunal Supremo español que se puede perpetrar un abuso sexual *stricto sensu* en interacciones desarrolladas en un contexto exclusivamente telemático. Así, si no hacía falta contacto corporal, ahora tampoco proximidad física. En este sentido, el Tribunal Supremo es contundente al respecto al afirmar que "más allá de aquellos supuestos en los que la falta de contacto físico se produce en un contexto de proximidad entre agresor y

32 Sobre la naturaleza simulada del ciberespacio, véase POSADA MAYA, «El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual», *Nuevo Foro Penal*, 13(88), pp. 72-112; MEEK NEIRA, *Delito informático y cadena de custodia*, Universidad Sergio Arboleda, Bogotá, 2013, pp. 39-40.

víctima, las nuevas formas de comunicación introducen inéditos modelos de interrelación en los que la distancia geográfica deja paso a una cercanía virtual en la que la afectación del bien jurídico, no es que sea posible, sino que puede llegar a desarrollarse con un realismo hasta ahora inimaginable"[33].

Da lo mismo, pues, estar a 3.000 kilómetros. La lesión del bien jurídico es idéntica en ambos casos[34]. La misma corporeidad en los delitos sexuales parece haberse convertido en un mero accidente, tocando a través del teclado la sexualidad de la víctima tan solo de forma virtual (*strumming my pain with his fingers*). ¿Qué se está lesionando entonces si se puede agredir sexualmente a la víctima desde la otra punta del globo?

En las líneas que siguen, a partir del referido análisis sobre las repercusiones antropológicas y el cambio de paradigma en el modo de cometer/padecer delitos, se pretende justificar un nuevo enfoque desde la teoría del delito que permita afrontar algunos retos que plantea la cibercriminalidad. Ese nuevo enfoque debería integrar las tres perspectivas: criminológica, dogmática y procesal, de modo que el sistema parta de la realidad y sea funcional en la resolución de problemas y en la práctica probatoria.

La teoría jurídica del delito no debería –esa es nuestra principal aportación– prescindir del conocimiento antropológico y criminológico del *ser-humano-mediado-por-la-tecnología*; ni tampoco dejar de considerar en qué se traduce la

33 STS núm. 301/2016, de 12 de abril (ponente Marchena Gómez).

34 No obstante, se plantean numerosos interrogantes en esa supuesta plena equiparación (desvalorativa y penológica). Por ejemplo, a efectos de valoración del daño, ¿da lo mismo sufrir un atentado contra la libertad o indemnidad sexual offline que online? Sobre este punto, volveremos más adelante en el cuerpo del texto. De lo que no cabe duda es de que el nivel de ansiedad y otras repercusiones psicológicas de una víctima online se puede ver notablemente afectado por el miedo a una potencial re-victimización permanente: una vez se han plasmado en soporte digital las imágenes, la tranquilidad emocional por parte de la víctima es mucho más difícil de gestionar.

modulación en las categorías y estructuras de imputación en el ámbito de la prueba. Se formularán a continuación las bases y principales argumentos que justifican ese nuevo enfoque dogmático e integrador para afrontar los retos que plantea al sistema la cibercriminalidad, dejando su completo desarrollo para futuros trabajos.

3. Bases para una teoría del delito adaptada a la era digital

Llegados a este punto, en concreto, ¿qué supuestos cambios ha generado la revolución tecnológica y la cibercriminalidad que deban tenerse en cuenta en la arquitectura conceptual y en las categorías dogmáticas de la teoría del delito? Es decir, ¿algún cambio esencial en las circunstancias obligaría a ajustar un cambio en las estructuras de imputación penal? Si, en efecto, nos hallamos ante un momento decisivo de transición del concepto tradicional de Derecho penal, que requiere, entre otras tareas, una renovación siquiera parcial de la teoría tradicional del delito, ¿en qué se traducirían tales cambios y cómo se justificarían? ¿Qué metodología debería seguirse a tal fin?

Mi tesis es que un cambio significativo en la realidad empírica[35] sí puede producir, sin alterar lo esencial, algunas

35 Por realidad empírica me refiero aquí a todo aquello que precede a la realidad normativa (no solo jurídico-positiva). Incluiría, pues, las condiciones de posibilidad del desarrollo del ser humano, su *modus vivendi*, así como los valores culturales y sociales que le circundan. Englobaría, por tanto, al hombre en su dimensión psicológica, cultural y antropológica aquí y ahora. Ese contexto es el marco en el que se deben analizar los contenidos de deber jurídicos (y no solo jurídicos, también morales). No es posible detenerse aquí con mayor profundidad sobre la discusión entre ser y deber ser, ni sobre las implicaciones mutuas entre ambos mundos. La dogmática debería acoger esa realidad e interaccionar con ella. De conformidad con mi posición, habría unos principios normativos inmutables y otros "principios" (o si se prefiere, sub-principios o incluso reglas: no tengo claro a qué nivel se encontrarían) surgidos de la experiencia que, aquí y ahora, modularían los primeros.

modulaciones importantes en las categorías y estructuras de imputación de la responsabilidad penal. No solo la política criminal necesita apoyarse en estudios empíricos[36]. Los principios abstractos formulados por la dogmática penal deben abrirse a la realidad social y tener vocación de aplicabilidad, pues, de otro modo, *no servirían para nada*. Están llamados a aplicarse y convertirse en principios "encarnados", cuanto más tangibles y mensurables, mejor. Sin embargo, el lenguaje dogmático ha abusado de un excesivo formalismo, en particular por la influencia del funcionalismo y la teoría de sistemas aplicada al Derecho penal.

En este punto resulta determinante la relación entre Derecho penal y Criminología. Si bien la dogmática tradicionalmente ha dado la espalda a la Criminología, se ha avanzado en la apertura del sistema hacia la realidad social, no solo en relación a los estudios sobre la necesidad y efecto disuasorio de las penas. Una dogmática atenta a las investigaciones empíricas es necesaria a los efectos de "traducir en estructuras categoriales y sistemáticas" las valoraciones efectuadas desde un plano político criminal[37]. Esta cuestión, no obstante excede el objeto principal de este trabajo[38].

---

36 Por todos, DÍEZ RIPOLLÉS, *La racionalidad de las leyes penales*, Madrid, Trotta, 2003.

37 SILVA SÁNCHEZ, *Aproximación al Derecho penal contemporáneo* (2ª ed.), BdeF, 2010, p. 157 y ss.

38 Así, por ejemplo, se puede construir en abstracto una institución como la legítima defensa y desarrollar una serie de reflexiones axiológicas sobre si es justo o proporcional justificar y eximir total o parcialmente en determinados casos a una persona que se ha visto agredida. Se pueden describir distintos grupos de casos también en abstracto. Pero no se puede desconocer cómo funciona en la práctica el ser humano condicionado por un contexto psicológico o cultural determinado. Por ejemplo, ¿qué efectos fisiológicos produce una situación de amenaza en quien se dispone a defenderse? ¿Está operando la jurisprudencia con criterios ideales que en nada se aproximan al sujeto de carne y hueso? Sobre la contracara de los constructos normativos, véase, GARCÍA AMADO, "Anatomía de un imposible. La imagen jurisprudencial del policía", 2003, en DOMÍNGUEZ/GARCÍA AMADO/HEBBERECHT/RECASENS

A este respecto, suele afirmarse que la Criminología y el Derecho penal persiguen finalidades radicalmente distintas (aunque compartan objeto) y parten de prismas valorativamente no compatibles (el mundo empírico del ser *versus* el reino normativo del deber ser)[39]. Se sostiene, en este sentido, que lo que puede venir bien a una (reducir el delito), no siempre sirve a los fines del otro (proporcionar una respuesta justa). No obstante, este discurso (algo maniqueísta) no permite, entre otras cosas, *esponjar* la dogmática con información de la realidad, de una realidad que es necesaria, precisamente, para cumplir esa función de justicia en el caso concreto que ella misma pretende[40]. La premisa principal de la que parte la

(eds.), *La seguridad en la sociedad del riesgo*, Madrid, Atelier, 2003, pp. 181-200, en donde critica que la imagen jurisprudencial de la policía confiera una "capacidad para ser ponderador de precisión", cuando no siempre sucede así. Con frecuencia, necesita el andamiaje dogmático de un cierto "baño de realidad" para no poner en jaque su función esencial: dotar al sistema de estructuras de imputación que sean trasladables a la realidad en condiciones de racionalidad, previsibilidad y seguridad. Sobre la tensión e inadaptaciones entre la solución de la cuestión de hecho y las exigencias sistemáticas, JESCHECK/WEIGEND, *passim*, p. 210-211.

39 SILVA SÁNCHEZ, *Aproximación*…, 2010, p. 154, donde enfatiza que en una dogmática orientada a fines las decisiones centrales siguen siendo valorativas: en tanto que del ser no deriva el deber ser, los resultados de la investigación criminológica pueden dar lugar a decisiones valorativas distintas (e incluso contrapuestas) en función de las premisas axiológicas de partida. En el mismo sentido, BERISTAIN (1985), *Ciencia penal y Criminología*, pp. 38-39.

40 Véase, BOTTOMS, "The relationship between theory and empirical observations in criminology". En R.D. King/E. Wingcup, *Doing research on crime and justice*, Oxford University Press, 2008, pp. 75-116, donde señala que el razonamiento normativo implica contestar a la pregunta "¿Debería…?", para lo cual no significa que no puedan invocarse conocimientos empíricos. Como señala LARRAURI, el problema reside en un estudio del derecho excesivamente formalista, que no atiende a la realidad ni a las consecuencias (LARRAURI, *Introducción a la Criminología y al sistema penal*, Trotta, 2015, p. 28). A mi juicio, el problema es el punto de partida, ese formalismo simplista que pretende alcanzar una dogmática perfecta, inmune a las impurezas externas. El ser humano

dogmática es la acción humana y esta no es inmutable, sino que históricamente puede sufrir, y sufre, modulaciones significativas en aquellos elementos básicos que son la base de su posterior interpretación. La acción se construye sobre ciertas condiciones de posibilidad, en un contexto determinado que es preciso examinar con atención, pues del concepto de acción se deriva todo. La teoría de la acción es "punto de referencia para los predicados de la tipicidad, antijuricidad y de la culpabilidad"[41], sin perjuicio de que la "suerte de la dogmática penal" se juegue solamente en esos niveles posteriores de la investigación de un comportamiento[42].

Todas estas reflexiones deberían proyectarse en última instancia, como no puede ser de otra forma, sobre concretas figuras de delito en su aplicación a una realidad cambiante, pues las categorías dogmáticas no son constructos abstractos desgajados de la realidad: son conceptos cargados de realidad, imprescindibles en la gramática que emplea el Legislador

---

y toda su complejidad es incompatible con un dogmatismo centrado en la ortodoxia y coherencia lógica de un sistema que se pretende no solo autopoyético, sino que excluye la importancia del enfoque sociológico del Derecho penal y una cierta apertura a ciencias "extrañas". La disonancia sería insoportable si se pretendiera construir y encapsular en compartimentos absolutamente estancos la teoría (jurídica) del delito, la teoría de la prueba y la teoría (criminológica) del ser-humano-que-comete-un-delito. En el contexto de la postmodernidad, se debería tratar de reconstruir la dogmática permitiendo que entre (aporte criminológico) y salga (filtro probático) esa realidad de carne y hueso que los principios inmutables parecían esconder. Necesitamos, pues, una "nueva" dogmática que sea más permeable y aspire a una integración lograda de las tres teorías. Esta tarea, no obstante, es ingente. Aquí nos limitaremos a poner el foco en una parcela: cómo el nuevo contexto tecnológico ha provocado una mutación en el concepto de acción y bien jurídico, una adaptación de las reglas de imputación objetiva y una reconfiguración de algunas posibles limitaciones cognitivas y volitivas de ese ser humano constreñido por lo tecnológico.

41 Véase, JESCHECK/WEIGEND, *passim,* p. 234 y ss.

42 Así, SCHÖNKE/SCHRÖDER/LENCKNER, nota preliminar núm. marginal 37, comentario preliminar al § 13 (citado en JESCHECK/WEIGEND).

a la hora de tipificar concretas conductas humanas sobre un substrato en parte inmutable, *pero en parte cambiante*. Tales conductas lesionan, en todo caso, un bien jurídico y traspasan los umbrales de relevancia para preservar la convivencia pacífica en un mundo que, al menos hasta hace tan solo unos años, se había concebido en términos predominantemente físicos[43]. La función de la pena como comunicación simbólica[44] posee connotaciones importantes también en la arquitectura del ciberespacio, donde se produce una virtualización de los bienes jurídicos. Y no solo la pena; también el delito es, ante el nuevo paradigma relacional que plantea el ciberespacio, sobre todo y más que nunca, comunicación, sin perjuicio de que pueda tener efectos en el sustrato físico-corporal de la víctima. Sobre este punto, volveremos más adelante al tratar sobre el proceso de virtualización del bien jurídico.

De tales cambios contextuales, un ejemplo paradigmático es el de la dogmática de la tentativa a la luz de los nuevos escenarios que plantea el ciberespacio. Como ya se apuntó en un trabajo anterior[45], la utilización de agentes encubiertos en la lucha contra la explotación sexual de menores en el ciberespacio rompe las condiciones espaciales y

---

43 La teoría (jurídica) del delito, en tanto que estructura conceptual que pretende facilitar el análisis normativo de la realidad delictiva, sirve con vocación de permanencia a la función de dotar de una mayor previsibilidad y seguridad a los operadores jurídicos en la tarea de interpretar las categorías dogmáticas y, en última instancia, los tipos penales (JESCHECK/WEIGEND, *Tratado de Derecho penal*, 2002, pp. 210-211).

44 Al respecto, JAKOBS, *Sociedad, norma y persona en una teoría de un Derecho penal funcional,* 1996. La tesis del funcionalismo normativista dio un paso a la hora de entender la infracción de la norma (delito) y su respuesta (pena) como comunicaciones de sentido, visión que todavía cobra mayor expresividad en el contexto del ciberespacio.

45 Véase AGUSTINA/VARGAS OVALLE, "¿Es necesaria una dogmática de los ciberdelitos? A propósito de la utilización de agentes encubiertos en la lucha contra la explotación sexual de menores en el ciberespacio". En *Derecho penal y persona* (coord. GARCÍA CAVERO/CHINGUEL RIVERA), 2019, pp. 609-644.

culturales sobre las que se edificaba la discusión sobre la tentativa relativamente inidónea.

En el caso objeto de examen, se analizó cómo desde una ONG se combatía (y se combate) de forma proactiva el turismo sexual infantil vía webcam mediante la utilización de un avatar denominado 'Sweetie', con el fin de identificar a *groomers* en busca de víctimas en el ciberespacio. Así, tras la apariencia de una niña filipina virtual de 10 años, un agente de dicha organización empezó a recoger información de las personas que iban contactando con Sweetie, y a poner dicha información en conocimiento de las autoridades de los distintos países para iniciar distintas investigaciones. El problema radica en que tanto la doctrina como la jurisprudencia rechazan de forma tajante la punibilidad de todos los casos de tentativa inidónea por *inexistencia de objeto*, y ello a pesar de que cualquier hombre medio vería como peligroso *ex ante* el acercamiento e interacción de un *groomer* con un avatar con forma de niña. No obstante, como ya expusimos, de acuerdo con la teoría de la impresión, la alarma social que genera este tipo de delitos (imposibles) y la necesidad de proteger a los menores de edad debería justificar una revisión de este tipo de escenarios[46].

Pues bien, esa nueva justificación (del cambio doctrinal y jurisprudencial respecto al delito *imposible*), obedecería, en realidad, a un cambio mucho más profundo. El hecho de que Internet se vea inundado de avatares con apariencia de seres humanos genera algunos problemas dogmáticos y procesales. En un mundo en el que la distinción entre lo real y lo simulado es constante, en el que nuestro yo-real se

46 AGUSTINA/VARGAS OVALLE, "¿Es necesaria una dogmática…?", *passim*. En dicho trabajo se da cuenta también de las dificultades de delimitación entre algunas formas de ciberpatrullaje legítimo y los casos de delito provocado. El policía de paisano que frecuenta una zona de menudeo y tráfico de drogas y al que le ofrecen comprar, no provoca el delito y, aun siendo legítima su actuación, no deja de ser una trampa de los órganos del Estado.

proyecta sobre un potencial número de yoes-digitales sin aparente límite, los bienes jurídicos protegibles no abarcarían solo un bien jurídico vinculado directamente a un sustrato corpóreo, sino que alcanzaría a toda una serie de identidades digitales construidas. La criminalización de la pornografía virtual también se apoya sobre un cambio de paradigma. Cuando se envía por Internet una solicitud sexual indiscriminada (como cuando se produce un envío masivo de correos electrónicos maliciosos con la intención de engañar), se está poniendo en serio peligro un espacio que normalmente es transitado por personas y en el que las expectativas sociales exigen, a priori, que la representación se corresponda con la realidad. Por todo ello, la peligrosidad es intolerable[47], a pesar de que el bien jurídico sea virtual, es decir, aparente o potencial, pero no real[48]. En tal contexto, la inexistencia de objeto real deviene irrelevante: lo único que cuenta es lo aparente, pues esas son las reglas de Internet.

Así las cosas, el cambio de percepción individual y social conlleva que, más allá de la teoría de la impresión, el bien jurídico se ha llegado a transformar, pudiendo hallarse en algunos casos totalmente virtualizado. Por ejemplo, ¿qué pasaría si los ataques se dirigieran contra el perfil de un menor en una red social que estuviera en desuso temporal o definitivamente? ¿Y si detrás de la apariencia de un menor se escondiera un adulto?

---

47 O podría no serlo si se modificara la arquitectura del ciberespacio, reduciendo el anonimato y elevando los niveles de transparencia y vigilancia. Es parte del binomio que atraviesa buena parte de la política criminal: a mayor privacidad, menor seguridad.

48 En la voz "virtual" del Diccionario de la Real Academia Española se recoge: "Del lat. mediev. virtualis, y este der. del lat. virtus 'poder, facultad', 'fuerza', 'virtud'. 1. adj. Que tiene virtud para producir un efecto, aunque no lo produce de presente, frecuentemente en oposición a efectivo o real. 2. adj. Implícito, tácito. 3. adj. Fís. Que tiene existencia aparente y no real. 4. adj. Inform. Que está ubicado o tiene lugar en línea, generalmente a través de internet" (https://dle.rae.es/virtual).

Asimismo, señalaba en ese trabajo –y reproduzco aquí, habiendo añadido ciertos matices– algunas cuestiones a modo de ejemplo que convendrá analizar con más detenimiento en el futuro.

1. Frente a lo analógico, la realidad digital puede plantear adaptaciones importantes en la teoría de concursos, en el *iter criminis* o en la ya referida dogmática de la tentativa. ¿El solo envío de un *scam* indiscriminado supone el inicio de una tentativa múltiple? En el ciberespacio resulta más difícil separar en secuencias espacio-temporales, rompiendo la unidad de acción. Con un solo *click* todo se consuma (sin discontinuidad) y al mismo tiempo todo se perpetúa, pudiéndose replicar el injusto o multiplicarse automáticamente, quizá mediante la intervención de terceros ajenos (piénsese en la propagación en cascada de un virus con efectos heterogéneos).

2. En cuanto a situar el inicio/final del hecho, ¿qué implicaciones tiene en el binomio delito permanente *versus* delito instantáneo la disponibilidad de acceso *sui generis* de las noticias o de los mensajes en redes sociales? En Internet, se produce una publicidad real multiforme (a veces latente, en ocasiones gradual o discontinua, y muchas veces caprichosa, con motivo de la viralización del mensaje), pero accesible *sine die*, que puede presentar problemas a los efectos de fijar el inicio el cómputo del plazo de prescripción en un delito de injurias cometido en el ciberespacio. ¿Cómo afecta a las fases del *iter criminis* y a la teoría de concursos la sucesión y/o alternancia de comportamientos *offline* y *online*, por ejemplo, en los delitos de *online grooming* seguidos de abuso sexual virtual?[49]

49 El delito del art. 183.ter está pensado sobre la base de que, tras el contacto telemático, el acercamiento deba producirse en el espacio físico. ¿Qué sucede si el contacto sexual se virtualiza, tal y como admite ya la jurisprudencia (por todas, STS núm. 301/2016, de 12 de abril)? No parece que en los casos de abuso sexual online sea aplicable lo dispuesto en el Acuerdo del Pleno No Jurisdiccional de la Sala Segunda del Tribunal

3. La proyección del dolo sobre realidades virtuales puede ser un campo abonado para situaciones de engaño/ignorancia/error que, con más frecuencia, justifique unos estándares de diligencia diversos a los usuales en el mundo offline. Un octogenario acusado de difundir pornografía infantil puede alegar que desconocía que sus archivos estaban siendo utilizados por terceros, pues no sabía que el programa P2P permitía esa posibilidad. El sujeto activo no puede calibrar si su engaño es burdo o bastante porque no puede representarse a sus potencialmente miles de interlocutores. ¿En qué consiste y cómo se modula (si es que lo requiere) la exigencia de *engaño bastante* en las interacciones online, en las que los comportamientos compulsivos provocan una minoración de los estándares de autoprotección? ¿Es solo una cuestión de interpretación del tipo o requiere un análisis dogmático más profundo sobre el error y/o el consentimiento en la era actual? Es indudable que el ciberespacio ha alterado de alguna forma la concreción de los deberes de veracidad, así como los deberes de autoprotección de la víctima.

4. Por contraposición, la participación *ambiental* en el delito puede multiplicarse rápidamente (deviniendo impracticable su persecución) o llegar a convertirse en participación accesoria, que opere con independencia de conocer el autor el alcance real de la audiencia (la subida de adrenalina le bastaría como refuerzo psicológico). Entre otras cuestiones, ¿cómo se debería analizar la participación en el delito de los *mirones* o "by-standers" cuando se omiten deberes de socorro o de denuncia en delitos cometidos en el ciberespacio en los que concurre una cierta dependencia del bien jurídico respecto del omitente? ¿En qué situaciones las plataformas o los intermediarios (*Internet Service Providers*) pueden ostentar ciertas posiciones de garantía penalmente relevantes? ¿Cuál es el *equivalente funcional* en el ciberespacio de la posición de

Supremo de 08-11-2017, que se decanta por el concurso real con los delitos posteriores al grooming.

garante derivada de un dominio sobre el espacio en el que se comete un delito en el mundo físico?

5. La dogmática del consentimiento podría ofuscarse (¿quién consiente y a qué?) o someterse a otras reglas. Por ejemplo, ¿qué significa consentir en el lenguaje de las redes sociales si, por ejemplo, en el perfil de Twitter del acusado se explicita que "RT ≠ endorsement"? ¿Debe ser punible siempre la acción de *retuitear* algo ajeno en los delitos contra el honor o de incitación al odio?[50] Y en los delitos contra la intimidad, ¿caben formas distintas de "implied confidentiality"[51] en el mundo digital en los que jueguen indicios de consentimiento presunto distintos a los que pueden darse en el mundo físico?

6. ¿Seguirá vigente y sin alteraciones el principio de impunidad de la mentira y la preeminencia del modelo de la estafa[52] en el escenario actual de posverdad, *fakenews* y libertad de expresión que potencia Internet, o se irán abriendo nuevas formas delictivas? Sin duda, en el debate sobre la criminalización de la creación y difusión de *fakenews* serán necesarios aportes dogmáticos que restrinjan el alcance del tipo.

7. ¿Qué incidencia tiene en la teoría del bien jurídico la realidad virtual o aumentada? ¿Cómo se configura el equivalente funcional del contacto corporal en el ciberespacio? ¿Debería corregirse la doctrina jurisprudencial

50 Véase, STS 706/2017, de 27 de octubre. En las redes sociales, las particularidades del lenguaje pueden dificultar la interpretación, o diluir el sentido, por ejemplo, si se unen diversos mensajes o se utiliza una mezcla de expresiones escritas o gráficas de elaboración y autoría propia con otras ajenas al usuario y que éste comparte.

51 Sobre esta cuestión, véase, HARTZOG, "Reviving Implied Confidentiality", *Indiana Law Journal* 89 (2014), pp. 763-806.

52 SILVA SÁNCHEZ, "Las inveracidades de los particulares ante el Derecho penal". En *Simulación y deberes de veracidad. Derecho Civil y Derecho Penal: dos estudios de dogmática jurídica,* SALVADOR CODERCH/ SILVA SÁNCHEZ, Civitas, Madrid, 1999, p. 77 y ss.

de los delitos imposibles impunes por inexistencia de objeto, cuando la afectación a éste, aun siendo virtual, desencadene un cierto nivel de conmoción en la comunidad?

8. ¿Qué estructuras de imputación nuevas, en términos de autoría y participación, podrían darse cuando intervengan inteligencias artificiales? ¿Y, en términos de justificación, por ejemplo, qué adaptaciones se requerirán ante la resolución programada de colisiones de deberes que deberán afrontar, por ejemplo, coches autopilotados y otras inteligencias artificiales?[53]

Estos ejemplos ponen de manifiesto la necesidad no solo de buscar soluciones interpretativas a los tipos penales existentes, sino también (y, sobre todo) de repensar o cuando menos adaptar algunas categorías del delito a la era digital. La jurisprudencia y la doctrina no pueden discurrir sin introducir en su análisis elementos novedosos importantes como los reseñados. Y desde el punto de vista procesal-probatorio, no cabe duda que la prueba digital posee un rol cada vez más importante en las valoraciones del órgano sentenciador y que resulta inaplazable un mayor desarrollo de conceptos y categorías procesales tradicionales, adaptándolas a un contexto en el que las TIC son determinantes. Piénsese, por ejemplo, en el criterio de ubicuidad, en las afectaciones al derecho a la intimidad en diligencias de entrada y registro, en la doctrina del hallazgo casual o en los criterios para determinar la autoría cuando el sospechoso ha empleado un dispositivo electrónico o ha sido geolocalizado, etc.

53 Así, la configuración programada de cómo resolver una colisión de deberes en coches autopilotados se enfrenta a dilemas de difícil solución, como el expuesto por Coca Vila, en el que, a consecuencia de un fallo imprevisible en el sistema de frenado, un vehículo autopilotado solo puede salvar la vida de su único ocupante invadiendo la acera, donde camina un peatón que, con toda seguridad, morirá como consecuencia del atropello (en extenso, COCA VILA, "Coches autopilotados…", 2017).

4. Sobre el concepto de ciberdelito y su función en el marco de la teoría dogmática

La definición de qué se entiende por ciberdelito (o cibercrimen[54]) ha generado controversia debido en parte a la falta de claridad en la naturaleza y función del constructo, dando lugar a distintas y muy variadas aproximaciones y clasificaciones[55].

54 MIRÓ ha descrito la evolución de la terminología empleada en lengua española en el ámbito de los delitos cometidos en el ciberespacio, describiendo diversas etapas desde la delincuencia informática a la cibercriminalidad. En el origen del concepto "delito informático" se tenía en cuenta tanto el medio utilizado (herramientas tecnológicas o procesos electrónicos), como el objeto de ataque (sistemas informáticos) (MIRÓ, *El cibercrimen*…, p. 33 y ss.). Sin embargo, los medios o el objeto del delito nunca se circunscriben exclusivamente a una realidad digital. En los ciberdelitos, la tecnología es simplemente el lugar o medio comisivo principal o determinante para explicar el evento delictivo. En lengua inglesa se han ido empleando diversos términos (*computer crime o computer-related crime, digital crime, e-crime, online crime*, entre otros). Desde la década de 1990 empezó a coger fuerza el término 'cybercrime', siendo actualmente el más utilizado (LAVORGNA, *Cybercrimes*, 2020, p. 16).

55 Sobre el concepto de ciberdelito, desde una perspectiva más criminológica, CLOUGH, *Principles of cybercrime*. Cambridge University Press, 2015, pp. 9-12; MIRÓ, *El cibercrimen*…, p. 33 y ss.; WALL, "Cybercrimes and the Internet". En D.S. Wall (ed), *Crime and the Internet*, New York: Routledge, 2001, pp. 1-17; LAVORGNA, *Cybercrimes*, 2020, pp. 13-18; AGUSTINA/MONTIEL/GÁMEZ, *Cibercriminología y victimización online*, 2020, p. 34 y ss.; GILLESPIE, *Cybercrime: key issues and debates*. Routledge, 2019, pp. 1-20; HOLT/BOSSLER/SEIGFRIED-SPELLAR, *Cybercrime and digital forensics: An introduction*. Routledge, 2015, p. 21 y ss. Desde un punto de vista jurídico-penal, para algunas definiciones muy diversas de ciberdelito o derecho penal informático, véase, ABOSO, *Derecho penal cibernético*, p. 3; HERNÁNDEZ DÍEZ, Aproximación a un concepto de Derecho penal informático, en DE LA CUESTA ARZAMENDI/DE LA MATA BARRANCO, *Derecho penal informático*, p. 31 y ss.; MATA Y MARTÍN, "Criminalidad informática: una introducción al cibercrimen", *Actualidad penal* 37 (2003): 935-961; POSADA MAYA, «El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual», *Nuevo Foro Penal*, 13(88); ROMEO CASABONA, "De los delitos informáticos al cibercrimen: una aproximación conceptual…", pp. 1-43; VELASCO NÚÑEZ, *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Sepin, 2016, p. 175 y ss.

El origen del problema, a mi juicio, se halla (en parte, al menos) en la errónea interpretación de la clasificación en diversos grupos de ciberdelitos que se utilizó sin ulteriores pretensiones en el Convenio del Consejo de Europa sobre Ciberdelincuencia (Budapest, 2001).

No cabe duda de la aportación fundamental que significó dicho instrumento normativo internacional, al suponer la incorporación obligatoria por parte de los Estados signatarios de un listado de tipos penales mediados por la tecnología que permitieran una lucha conjunta en un mundo global y en un proceso de digitalización exponencial. Con todo, lo único a que obligaba dicho tratado (en relación a las figuras delictivas que recogía) era a incorporar un grupo de tipos delictivos (descritos de modo no pormenorizado), pero sin exigir la concreta forma de integración de los mismos en los respectivos códigos de los Estados firmantes.

En el cuerpo de dicho convenio se diferenciaba entre (1) delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (Título 1) y (2) delitos informáticos (Título 2), añadiendo a modo de cajón de sastre en un tercer grupo (3) los delitos relacionados con el contenido y las infracciones de la propiedad intelectual y derechos afines (Títulos 3 y 4). *Prima facie*, solo los delitos del Título 1 se agrupan bajo un mismo bien jurídico (la seguridad o funcionalidad informática[56]) como criterio rector. No obstante, en realidad, junto a la seguridad de las funciones informáticas se acaba lesionando otros bienes jurídicos,

56 A tenor de lo establecido en el convenio, el bien jurídico tendría que ser la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. La doctrina trata de unificar esa diversidad de propiedades de la información y comunicación digitales, agrupándolas en el término seguridad (por ej., Posada Maya) o funcionalidad (Mayer Lux). Véase, respectivamente, POSADA MAYA, *Los cibercrímenes: un nuevo paradigma de cibercriminalidad*, Universidad de los Andes, Colombia, 2017 y MAYER LUX (2017). El bien jurídico protegido en los delitos informáticos. Revista chilena de derecho, 44(1), 261-285.

como la intimidad o privacidad de los datos, el patrimonio o los secretos de empresa. Incluso el mero acceso ilícito por parte de hackers éticos a un sistema informático (por puro divertimento) también pone en peligro la privacidad de los datos albergados en ese sistema. Son, pues, delitos informáticos de carácter *instrumental* que, en definitiva, solo se entienden en su plenitud a la luz del delito-fin que persiguen.

Con base en esa clasificación, con diversa terminología y, en ocasiones, cierta confusión, se ha tratado de diferenciar en la doctrina, desde un punto de vista jurídico, entre "delitos informáticos" en sentido amplio (los recogidos en el Título 2) y delitos informático en sentido estricto o "cibercrímenes" (los recogidos en el Título 1)[57]; o, desde una perspectiva criminológica, entre o "cibercrímenes réplica" (aquellos que tienen una figura delictiva tradicional equivalente) y "cibercrímenes puros" (los que solo afectan a una dimensión virtual del bien jurídico y se corresponderían con los delitos informáticos en sentido estricto)[58]. Sin duda, tales dicotomías pueden tener sentido y utilidad práctica. Desde un punto de vista jurídico, por ejemplo, esa distinción puede ser orientadora para analizar qué elementos propios del ciberdelito son exigibles adicionalmente (con respecto a la modalidad tradicional), o cómo debe tratarse la relación de concurso medial entre ambos tipos de delitos, pues los ciberdelitos del Título 1, como señalamos, siempre van a lesionar algún bien jurídico adicional a la seguridad informática.

Lo relevante, a mi juicio, es comprender que la clasificación utilizada en el Convenio de Budapest y la distinción que luego se derivó del mismo entre cibercrímenes y delitos informáticos no poseía efectos vinculantes, ni estaba imponiendo un modelo concreto de tipificación de los ciberdelitos. Tampoco implicaba un posicionamiento criminológico. Con

57 Sobre esa distinción, en sentido crítico, véase POSADA MAYA, *Los cibercrímenes*…, p. 99 y ss.

58 Véase al respecto, MIRÓ, *El cibercrimen*…, p. 51 y ss.

el convenio se pretendía *simplemente* cubrir algunas lagunas de punibilidad y reforzar los mecanismos de cooperación internacional en una primera reacción jurídica ante el nuevo escenario que planteaba el cibercrimen. Desde el punto de vista de técnica legislativa, cada Estado podía (obviamente) regular los ciberdelitos como nuevas modalidades o subtipos junto a las correspondientes figuras de delito tradicional o, por el contrario, agruparlos en un título o capítulo diferenciado en el Código penal (o en una ley específica separada), dedicado en exclusiva a delitos cometidos a través de las TIC. Solo en este segundo caso tendría sentido, en parte, referirse a un nuevo bien jurídico que diera unidad a esa agrupación. No obstante, cuando el Convenio de Budapest recogió de forma ordenada (¡hace ya casi veinte años!) los distintos ciberdelitos, simplemente estaba enumerando con un cierto orden las medidas que cada Estado parte debía adoptar en derecho penal tecnológico sustantivo.

Hoy tenemos mucho más claro que no se pueden desgajar los delitos tradicionales (cometidos en el mundo físico) de los delitos en cuya comisión las TIC juegan un papel decisivo. Son muchas veces el mismo delito con ciertas particularidades por razón de los medios empleados (la tecnología), medios que entrañan una mayor peligrosidad. Pero ese elemento que agrava el desvalor global del injusto puede tenerse en cuenta mediante dos delitos autónomos unidos en un concurso medial de delitos o a través de la apreciación de una circunstancia agravante o la creación de subtipos con ciertas adaptaciones, algunas estructurales (como en el caso de la estafa informática[59]).

Sea como fuere, la función de clasificación de los ciberdelitos con el bien jurídico como criterio rector (seguridad

59 En atención a ese plus de desvalor que es inherente al uso de la tecnología, debería recogerse siempre una pena agravada en las modalidades de delitos tradicionales cometidos a través de las TIC. En este sentido, se debería modificar, a mi juicio, la pena asignada a la estafa informática del art. 248 del Código penal español.

informática *versus* bienes jurídicos tradicionales) no era decisiva. Cada Estado puede optar por el modelo de tipificación que más le convenza, teniendo cada opción sus ventajas e inconvenientes, sin necesidad de reconocer a la seguridad informática el status de bien jurídico merecedor de delitos autónomos agrupados en un título aparte. La clasificación de Budapest no es, pues, el criterio relevante para el análisis típico, sobre todo si nos enfrentamos, como es el caso, a tipos penales pluriofensivos, en los que se lesionan diversos bienes jurídicos que plantean retos importantes en materia concursal[60]. Piénsese, por ejemplo, en el nuevo delito del art. 197.7 del Código penal español. Al castigarse la difusión inconsentida de imágenes íntimas no solo se está atentando contra la intimidad de la víctima (bien jurídico que estructura nuestro Título X), sino que se lesiona también su honor e integridad moral, llegando incluso a impactar en su libertad sexual en casos de sexting. En efecto, la publicidad y difusión de las imágenes propiciada por la tecnología desborda la mera incidencia en la intimidad de la víctima (sobre todo teniendo en cuenta la pena irrisoria prevista por el legislador). A mi entender, las TIC no requieren títulos separados sino afinar los instrumentos de análisis de concursos de normas y delitos, como se verá más adelante[61].

A mi juicio, la diferenciación fundamental se encuentra en justificar la separación (veremos con qué finalidad) entre delito tradicional y ciberdelito, a pesar de que esa nueva

60 Sin perjuicio de que la función clasificatoria del bien jurídico sea un importante medio de ayuda en la interpretación: véase, JESCHECK/WEIGEND, *Tratado de Derecho penal*, 2002, p. 277.

61 Si bien el criterio de agrupación (tipificación aparte *versus* dentro de la criminalidad tradicional) tiene argumentos a favor y en contra, pienso que un argumento a favor de la tipificación conjunta es el de arribar a interpretaciones sistemáticas/coherentes (por ejemplo, si se considera la interpretación de la estafa informática, parece sensato desarrollarla en atención a la interpretación de la estafa y no desvinculada de aquella). Con todo, esta discusión pormenorizada excede el propósito y objeto del presente trabajo.

realidad híbrida avance cada vez más, y en verificar si el ciberespacio, frente al espacio físico, comporta un cambio *significativo* a efectos jurídicos o criminológicos. Que suponga un cambio, nadie lo duda: lo relevante es qué comporta a efectos prácticos ese cambio para que existan dos categorías distintas.

Volviendo al punto de inicio, la confusión reinante en las definiciones y clasificaciones del concepto de ciberdelito se debe a la distinta naturaleza y función a que obedecen. Respecto a la función, habría que determinar para qué se pretende construir un concepto de ciberdelito: con una finalidad predominantemente analítica, explicativa y/o clasificatoria; o más bien, enfocada a la adopción de un régimen jurídico distintivo, aplicado transversalmente o a un tipo penal en particular. Respecto a la naturaleza, es importante especificar desde qué perspectiva se está analizando el fenómeno (jurídico-positiva, criminológica, procesal o dogmática).

Por lo que aquí interesa, conviene partir de que cualquier delito en cuya comisión las TIC revistan una importancia significativa merece un análisis diferenciado (con respecto a la misma conducta cometida sin el recurso a medios tecnológicos). Ese análisis diferenciado, ya sea desde el punto de vista criminológico o jurídico, no debe comportar siempre, como hemos sostenido, una técnica legislativa o forma de tipificación *ad hoc*. Así, por ejemplo, el núcleo del injusto del delito de injurias puede ser el mismo en el mundo físico y en el ciberespacio. Lo distintivo podría recogerse a través de una modalidad agravada del tipo básico, en atención a los efectos multiplicadores (y graduables) en la comunidad virtual. El delito de daños informáticos podría regularse como subtipo del delito de daños, incorporando sus especificidades y formas de ataque particulares, propia del medio virtual. Este es el modelo empleado por el legislador español.

Así las cosas, conceptualmente, desde el punto de vista del catálogo de delitos sostengo que los ciberdelitos en cuanto categoría propia *no existen*. Ni son tipos penales en

concreto, ni tiene sentido agrupar ciertas conductas típicas que revistan determinadas características asociadas a la cibercriminalidad bajo un título o rótulo de cualquier índole en el código penal de un Estado. Entre otros motivos, porque (en el caso de los delitos comunes cometidos a través de las TIC) la supuesta razón sería efímera (todo avanza hacia la continua hibridación entre los mundos online y offline) y porque (en el caso de los ciberdelitos puros) el hipotético bien jurídico común (la seguridad informática) no deja de ser un bien inmediato[62], siempre ligado a otro, en el marco de una lógica de un delito-medio que, *volens nolens*, siempre acaba siendo fagocitado por el delito-fin. Insistimos: no es posible un delito de *hacking* sin una lesión mediata a la intimidad o privacidad; o un delito de daños informáticos, sin una ulterior afectación a bienes jurídicos tradicionales.

Los ciberdelitos no tienen entidad propia porque el ciberespacio es una *realidad simulada* que solo existe por referencia a una realidad ligada, en última instancia, a un sustrato personal ajeno al propio ciberespacio. Al final, se refieren a personas, físicas o jurídicas, en su dimensión individual o supraindividual, que existen más allá de lo virtual. A pesar de la transformación experimentada, los bienes jurídicos siguen siendo los de siempre: solo han cambiado las formas de ataque. Incluso la destrucción de información digitalizada, almacenada en la nube, sin aparente base física alguna, posee conexión directa con un lugar físico (un ordenador) y con la información o trabajo relativo a personas concretas. El valor de dicha información persiste con independencia de que se haya digitalizado o se posea en soporte físico. Los ciberdelitos, por tanto, no suponen una novedad tipológica en sentido

62 Los pocos ciberdelitos "puros" en los que, supuestamente, se solo protege la seguridad informática, están protegiendo de forma mediata otros bienes. Así, en las modalidades de daños informáticos o de hacking se vulneran el patrimonio, la libertad o la intimidad del sujeto pasivo. La novedad reside en el modo de atentar contra ese bien jurídico, a través de la intromisión informática.

radical. En definitiva, los ciberdelitos no son algo ontológicamente distinto a los delitos tradicionales[63], sin perjuicio de que hayan motivado la creación de tipos penales específicos (mejorando o empeorando la situación) o hayan requerido algunos ajustes o especificidades desde el punto de vista de la teoría (jurídica o criminológica) del delito. Bien, porque los factores explicativos del delito difieren online y offline, bien porque las estructuras de imputación tradicionales necesiten algunos ajustes o la utilización de equivalentes funcionales.

Sentadas las precedentes aclaraciones, desde mi punto de vista se pueden plantear a distintos niveles cuatro definiciones de ciberdelito. La primera (que acabo de desechar), haría referencia al ciberdelito como grupo homogéneo de figuras de delito en particular y se enmarcaría en la Parte Especial del Derecho penal (*definición penal*).

La segunda definición más inmediata o práctica de ciberdelito consistiría en el objeto de análisis probático de este fenómeno novedoso al Derecho procesal que suponen los delitos cometidos a través de las TIC (*definición procesal*). Su estudio separado se fundamentaría en las particularidades que presenta probar los delitos de siempre en contextos tecnológicos, salvando los problemas de búsqueda, obtención y preservación de evidencias digitales de conformidad con los principios y garantías procesales.

En la tercera definición ya entraríamos en el análisis fenomenológico en sí (*definición criminológica*). Aquí se plantearía qué es un ciberdelito en tanto que realidad (algo) distinta a un delito y por qué es necesario definirlo y estudiarlo de forma separada. La función de la Criminología no es otra que explicar los fenómenos delictivos para comprender los factores que los propician, su dinámica comisiva y los protagonistas que intervienen, con la finalidad de prevenir o reducir la criminalidad.

63 En el mismo sentido, LAVORGNA, *Cybercrimes*, p. 17.

El uso de la tecnología como medio comisivo relevante es lo que caracteriza a los ciberdelitos. Se pueden encontrar distintas posiciones en torno a la relevancia del componente *cyber* en la fenomenología delictiva: desde la preponderancia de los medios tecnológicos en el *modus operandi*, se llega a posiciones menos exigentes, en las que basta un protagonismo incidental, pero en parte decisivo. En este sentido, podríamos referirnos a delitos-cometidos-a-través-de-las-TIC. McGUIRE/DOWLING crearon una dicotomía interesante al distinguir entre 'cyber-enabled' y 'cyber-dependent' crime[64]. Los primeros podrían abarcar cualquier delito tradicional en el que la tecnología sea una herramienta que facilita su comisión, mientras que los segundos no podrían perpetrase sin la mediación de las TIC. Con todo, la tendencia hacia una realidad híbrida restaría utilidad a dicha discusión, centrando el debate en los factores explicativos, sean o no puros, mixtos o híbridos.

Siguiendo a CLOUGH, se pueden enumerar 6 rasgos definitorios de los ciberdelitos o cibercrímenes, en los que se resumen cómo la tecnología facilita la comisión de hechos delictivos y dificulta su persecución: (1) escalabilidad: la tecnología permite el encuentro entre múltiples potenciales ofensores y víctimas en una dimensión sin precedentes; (2) accesibilidad: la ubicuidad de la tecnología conlleva una facilidad de acceso en tiempo y espacio (físico) sin límites aparentes; (3) anonimidad: la tecnología habilita a los ofensores para esconder su identidad con un amplio abanico de posibilidades; (4) portabilidad y transferibilidad: la tecnología proporciona una enorme capacidad de almacenamiento de datos en espacios exiguos, pudiendo replicar y transferir esos datos de forma simple y sin pérdida de su calidad originaria; (5) globalidad: en contraposición al carácter territorial de las

64 McGUIRE/DOWLING, *Cybercrime: A review of the evidence: Summary of key findings and implications. Home Office Research Report 75* (2013). London: Home Office, October.

leyes penales, la cibercriminalidad ha cambiado el paradigma eliminando fronteras de cualquier tipo; (6) ausencia de guardianes capaces: el riesgo percibido de detección y persecución de infracciones delictivas se reduce considerablemente en el ámbito de la cibercriminalidad, planteando a la policía retos nuevos en los que el ciberpatrullaje (de carácter preventivo) y las técnicas de recuperación, preservación y validez de evidencias (de carácter reactivo) serán clave para lograr que los procedimientos judiciales lleguen a buen término[65].

Finalmente, en cuarto lugar, el ciberdelito –tal y como se sostiene en el presente trabajo– merecería ser estudiado desde el punto de vista de la teoría (jurídica) del delito (*definición dogmática*). Las características estructurales comunes y los problemas inherentes que presentan en la imputación de responsabilidad, podrían llegar a justificar (o no) su inclusión como definición tipológica para la Parte General (¿se podría explicar como un subtipo especial en los delitos de comisión activa?) o, cuando menos, un análisis pormenorizado de algunos problemas dogmáticos de especial incidencia en aquellos delitos mediados por la tecnología.

Salvo en la primera de ellas, cada una de las definiciones se ordena a un fin particular y se sustenta ante una necesidad funcional: explicar los equivalentes funcionales a los principios o categorías tradicionales en el espacio físico. La entrada y registro con acceso a dispositivos electrónicos tiene algo similar y algo distinto a la entrada domiciliaria pura y simple. En esencia, supone una intromisión ilegítima si no se observan unas normas procedimentales. Lo mismo sucede con el delito de injurias: en el ciberespacio se lesiona el mismo bien jurídico. Al margen de algunas particularidades típicas (por ejemplo, la publicidad que entraña la red), el resultado de injuriar es el mismo, pero las características de la acción y sus efectos difieren en parte, en ocasiones

65 CLOUGH, *Principles of cybercrime*. Cambridge University Press, 2015, pp. 6-9.

justificando algunas adaptaciones (por ejemplo, en los efectos temporales de la acción a efectos del cómputo del plazo de prescripción).

Solo la definición procesal implica un cambio radical de régimen con efectos duraderos, en tanto que las evidencias digitales siempre afectan a esa novedad inalterable del ciberdelito: su perpetración por medios distintos al espacio físico. Pero esa novedad en lo procesal justifica una permanencia, no así el resto de constructos. En unos años, *todos* los delitos se explicarán o se probarán con base en la suma de acciones y omisiones por medios físicos y virtuales. Las interacciones humanas serán completamente híbridas. En ese escenario, perdida la novedad del ciberdelito, carecerá de sentido referirse a una tipología distinta, tampoco desde el punto de vista de las estructuras de imputación. Por tanto, la necesidad de una dogmática del ciberdelito y de una subdisciplina llamada Cibercriminología, siendo actuales, tienen fecha de caducidad.

5. Hacia una propuesta de revisión de algunas categorías, subconceptos o estructuras de imputación de una teoría del delito adaptada a la era digital

Si, según se acaba de sostener, puede ser útil o necesario a la teoría del delito tener en cuenta la especificidad del ciberdelito para cumplir con sus fines de racionalidad sistemática, debería plantearse a qué categorías conviene una cierta adaptación, en la medida en que, en el contexto de los ciberdelitos, algunas categorías tradicionales (o algunos subconceptos en que estas se descomponen) podrían ver disminuidas su capacidad de rendimiento por razón de ciertas disonancias estructurales en el sistema.

La tarea podría ubicarse también en el marco de la dogmática de la Parte Especial. En realidad, la dogmática aplicada a la Parte Especial es análisis dogmático en sentido

propio. Los elementos comunes se proyectan irremediablemente sobre los particulares. Y, de hecho, muchos elementos típicos se configuran como conceptos transversales que se aplican a distintos delitos con distintas reglas interpretativas, pero con una cierta gramática común. Esa es, a mi juicio, la verdadera vocación de la dogmática del delito: permear los elementos de los tipos penales y suministrarles un contexto de sentido, una gramática suprapositiva, ayudando a los operadores jurídicos a interpretar la realidad más tangible y, en lo que aquí interesa, más intangible.

La dogmática evoluciona, pues, con los cambios sociales, filosóficos, epistemológicos y culturales. En las últimas décadas, hemos asistido a una normativización del dolo o a un proceso de espiritualización de la violencia, por poner algunos ejemplos. O en la dogmática aplicada a la pena, se ha acudido a la discusión de los equivalentes funcionales[66]. Las estructuras de la teoría del delito (y de la pena) se flexibilizan y adaptan a nuevos paradigmas, reflejados en la evolución del concepto de acción o en la finalidad de la pena. Del mismo modo, con la inmersión digital nos enfrentamos a una *virtualización del bien jurídico* que, como veremos, posee implicaciones importantes. En suma, la reflexión dogmática –no puede ser de otro modo– se ajusta a los cambios sociológicos que marcan las condiciones de vida de los seres humanos y sus relaciones comunitarias. Así las cosas, la repercusión del cibercrimen en la teoría del delito debería traducirse, en este sentido, en una reformulación de algunas categorías o instituciones dogmáticas, tal y como ya empieza a apuntar una parte de la doctrina[67]. *Mutatis mutandis*, sucede de

66 Por todos, SILVA SÁNCHEZ, *Malum passionis. Mitigar el dolor del Derecho penal*, 2018, p. 113 y ss.

67 Véase, al respecto, entre otros, POSADA MAYA, El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Nuevo Foro Penal*, 13(88) (2017), 72-112; MIRÓ, "La cibercriminalidad 2.0: falacias y realidades", En: *Derecho penal y nuevas tecnologías*. A propósito del título VII bis del Código Penal, Memorias 4,

algún modo algo similar a lo que Silva Sánchez describió al referirse a las adaptaciones que han debido introducirse en algunas instituciones dogmáticas de la teoría del delito ante las nuevas realidades delictivas, mucho más normativizadas, que nos ha traído la (nueva) delincuencia socio-económica[68].

Así, me propongo plantear algunos sustitutivos o equivalentes funcionales que, desde un punto de vista sistémico, ayuden a preservar la estructura dogmática. Desde el punto de vista de la tipicidad, en algunos delitos se han introducido equivalentes funcionales para paliar, por ejemplo, la ausencia de engaño y el correspondiente error cuando la posición de la víctima viene ocupada por una máquina. Así, en el tipo de estafa informática, se ha reemplazado la estructura tradicional engaño-error-disposición por una simple "transferencia no consentida" precedida de una "manipulación informática o artificio semejante". Parece evidente que el componente tecnológico ha provocado en este caso una mutación en la estructura tradicional del delito de estafa. Y que, para salvar el problema de la ausencia de engaño, se ha tenido que construir un equivalente funcional del mismo. Sin engaño, no hay estafa, salvo que se considere que utilizar un sistema automatizado suplantando al único titular autorizado equivalga a engañar. Hubiera sido más fácil, en realidad, subsumir en algunos casos la conducta como modalidad de robo con fuerza en las cosas (de hecho, así se solventaba en algunas resoluciones judiciales[69]). Así las cosas, solo cabe

---

Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda, 2016, pp. 55-117; AGUSTINA, Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. Cuadernos de Política Criminal, 114(III), (2014), pp. 143-178.

68 Véase, SILVA SÁNCHEZ, "Teoría del delito y Derecho penal económico-empresarial". En SILVA SÁNCHEZ/MIRÓ LLINARES, *La teoría del delito en la práctica penal económica*. La Ley, Madrid, 2013, p. 33 y ss.

69 Por ejemplo, véase SAP Sevilla 212/2013, ponente Sánchez García. La cuestión ha sido objeto de viva polémica en la doctrina y la jurisprudencia

acudir a una equiparación (art. 248.2: "También se consideran reos de estafa…"), mediante un equivalente funcional: se está engañando a una máquina que suple a un ser humano, cuando esto no es así (contraviniendo el mismo rótulo del Capítulo VI: *De las defraudaciones* y de su Sección 1ª: *De las estafas*).

Muy sucintamente, me referiré a continuación a las categorías, subconceptos o estructuras de imputación en las que, de conformidad con lo que he señalado, interesar profundizar desde una perspectiva dogmática, más allá de las posibles soluciones que pueda plasmar el legislador en los distintos tipos penales o encuentre la jurisprudencia a la hora de buscar paralelismos para colmar las exigencias del juicio de tipicidad.

5.1. Modulaciones en el concepto de acción y sus implicaciones dogmáticas

Desde un punto de vista fenomenológico, la acción humana a través del ciberespacio se ha visto modificada no solo en el espacio, sino también en el tiempo[70]. La inmediatez y la permanencia son dos características que, sin duda, poseen un impacto en la naturaleza del delito y sus efectos. El ciberespacio nos aboca a un concepto virtual de acción, en el

de los últimos años, y ello a pesar de la reforma operada por la LO 5/2010, que introdujo la referencia expresa al uso de tarjetas de crédito y similares en el art. 248.2.c) CP.

70 MIRÓ, "La oportunidad criminal en el ciberespacio", *Revista Electrónica de Ciencia Penal y Criminología* 7 (2011): 1-07, donde señala: "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 […], 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" (p. 8).

que la dimensión analógica ha sido sustituida o complementada por la dimensión digital en un mundo en el que, junto a tales cambios, la comprensión de la función del Derecho penal es cada vez más comunicativa y, por tanto, menos cognitiva. Si cometer un delito es emitir una comunicación de sentido, ¿deberían despreciarse las implicaciones que tiene la creación del ciberespacio y su posterior intensificación en la vida social?

Tres son las mutaciones significativas del cambio en el paradigma de acción. La acción ya no es medible ni puede acotarse de conformidad con los estándares tradicionales. En primer lugar, la mutación del *espacio* en la era digital ha traído, desde el punto de vista jurídico-procesal, el surgimiento del principio de ubicuidad[71]. En segundo lugar, la mutación del *tiempo* en un mundo virtualizado, debería forzar un replanteamiento de las unidades de valoración y medición del instituto de la prescripción y de la funcionalidad de los denominados delitos permanentes. Los delitos no empiezan y acaban con la misma lógica discursiva con que lo hacían antes de la era del ciberespacio y de las redes sociales. En ese sentido, en relación al problema planteado *supra*, se debería buscar una solución diferente a los criterios para fijar el inicio del cómputo y el momento de finalización de los delitos de injurias o de los delitos de odio en el ciberespacio[72].

71 El principio de ubicuidad, como criterio rompedor en la asignación de competencia jurisdiccional, fue reconocido en nuestro ordenamiento en el Acuerdo del Pleno de la Sala 2ª del Tribunal Supremo de 3 de febrero de 2005 en los siguientes términos: "El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa".

72 Obsérvese que, a diferencia de lo que sucede con el paradigma de delito permanente (detenciones ilegales y secuestros), lo más probable es que los efectos del hecho, por ejemplo, en un caso de injurias, estén fuera del control del autor. En todo caso, eso no quita que los efectos del ciberdelito puedan graduarse y llegar a ser muy graves, cuestión que debería considerarse en el ámbito penológico.

Y, en tercer lugar, la mutación espacio-temporal conduce a una alteración en el *unum*. El solapamiento y contracción de las dimensiones de espacio y tiempo deberían tener un reflejo en la teoría de la unidad y pluralidad delictiva o en las fases del *iter criminis*. Todo esto sugiere una profunda revisión desde la teoría del conocimiento aplicada a la teoría dogmática del delito.

En esa nueva gramática conceptual, la teoría del delito debe partir de una renovada teoría de la acción humana. A lo largo de los años de evolución histórica, el modo de entender el concepto de acción por parte de la teoría del delito ha venido adaptándose al devenir de la teoría del conocimiento y de los valores ético-normativos dominantes, sin perjuicio de que se puedan identificar unas constantes mínimas de forma invariable.

Así, la acción humana se concibió, en primera instancia, como un constructo natural perceptible por los sentidos, que respondía al paradigma del causalismo positivista (concepto causal de acción). Con el avance de las ciencias y de la filosofía de la acción, esa concepción naturalística se fue normativizando[73]. Con todo, el substrato del que se partía seguía siendo la acción humana en el mundo físico, aunque se aceptara que las expectativas jurídicas tuvieran un origen normativo y que, al menos en los delitos de omisión, lo perceptible por los sentidos se materializara en tales casos en una no verificación de los efectos físico-naturales esperados.

Pues bien, nuestra tesis es la siguiente. Tras el concepto causal, final y social de acción, hemos asistido a una profundización en un concepto normativo-comunicativo de acción que, sin duda, ha servido a los fines de interpretar realidades normativas vinculadas, de alguna manera, al mundo físico. No obstante, la traslación progresiva del actuar humano a un contexto virtual o tecnológico requiere dar un paso más. Las

73 JESCHECK/WEIGEND, *Tratado de Derecho penal*, 2002, pp. 233-239.

acciones humanas han dejado de transitar por medios físicos o analógicos para discurrir mediante una lógica y unos modos digitales que también son reales.

Conviene tener presente que el mundo físico y el mundo virtual constituyen, ciertamente, dimensiones distintas, pero de un mismo "mundo real". El hecho de que el ciberespacio sea una realidad simulada no implica que deje de existir. Los medios analógicos y los medios digitales dibujan en términos fenomenológicos formas de acción distintas pero que, en última instancia, responden a un obrar humano, ya sea de forma próxima o remota. En este sentido, se acuñó el concepto "meatspace" para contraponerlo al de "cyberspace", pero para resaltar que lo que distingue principalmente ambos espacios es la presencia del sujeto en carne y hueso, o mejor, *de cuerpo presente*, a pesar de que los efectos de esa relación a través del ciberespacio pueden llegar a incidir, en ocasiones, en la corporeidad de la víctima[74].

El debate sobre un problema adicional (ficticio) parece aproximarse en relación con el uso potencial de implantes que conectan el cerebro humano mediante un chip a un ordenador, a propósito del proyecto de Elon Musk, Neuralink[75]. Sea mediante una técnica u otra, ha sido una constante la tentación de adentrarse en la mente humana para conocer prospectiva o retrospectivamente las intenciones y pensamientos que alberga una persona sospechosa. Por ejemplo, a propósito del uso del polígrafo como mecanismo para detectar de forma inconsentida declaraciones mendaces. Con los avances en la línea del proyecto de Musk, podrían llegar a plantearse límites al principio *cogitationis poenam nemo*

74 PEASE, "Crime futures and foresight: Challenging criminal behaviour in the information age". In *Crime and the Internet* (pp. 30-40). Routledge, 2003.

75 Sobre Neuralink, véase, MUSK, "An integrated brain-machine interface platform with thousands of channels", *Journal of medical Internet research* 21.10 (2019): e16194.

patitur. Sin embargo, pensar no es decidir sin poder ir marcha atrás. El proceso interno del pensamiento humano ni es lineal, ni es nítido. En caso de acceder a la trazabilidad de los tres momentos de la fase interna del *iter criminis* (ideación, deliberación, resolución), ese último estadio en que consiste la resolución no será nunca definitivo. Para que pudiera atribuirse virtualidad a un supuesto inicio de la tentativa (los actos preparatorios punibles siempre requieren el concurso de dos personas), haría falta algo más. No parece posible que el ordenador pudiera identificar pensamientos-resolutivos-sin-marcha-atrás, entre otras cosas, porque ni uno mismo sabe muchas veces qué va a acabar haciendo ni por qué. Con todo, esa lectura del pensamiento humano desde fuera sí podría ser útil, por ejemplo, con carácter retrospectivo. Por ejemplo, para recabar indicios digitales de la previsibilidad o intencionalidad de una determinada acción.

5.2. Ajustes en el concepto de bien jurídico

Como es sabido, el concepto de bien jurídico ha entrado desde hace tiempo en *fase estacionaria* por su poca capacidad de rendimiento y la progresiva pérdida de fuerza expresiva. Esa pérdida de operatividad se fue haciendo cada vez más evidente tras una primera época de "cómoda convivencia con los procesos de despenalización"[76]. Sin embargo, el principio de lesividad, ofensividad o de exclusiva protección de bienes jurídicos responde también, en parte al menos, a la lógica (positiva) de proteger (si es necesario, penalmente) los derechos fundamentales de los ciudadanos frente a injerencias en la esfera jurídica garantizada por el Estado.

A este respecto, desde diversos ámbitos se ha propuesto la necesidad de una relectura de los derechos fundamentales, adaptando ese núcleo esencial a una era digital que ha modulado significativamente el contenido de prácticamente

76 SILVA SÁNCHEZ, No sólo bienes jurídicos, *InDret penal*, editorial número 3 (2019).

todo el haz de derechos[77]. Así, la intimidad en esta nueva era digital es algo sustancialmente distinto al original concepto decimonónico derivado del domicilio como refugio del yo; o el derecho a la presunción de inocencia en la sociedad del *big data* necesita ciertas adaptaciones, no menores[78]. Esos derechos digitales, en lo que aquí interesa, conformarían parte del contenido de los bienes jurídico-penalmente relevantes. Unos y otros, ubicándose en vasos comunicantes (cada uno con sus propios matices), necesitarían una revisión a la luz de la transformación digital experimentada.

En esta nueva era de expansión y posmodernidad penal, la dogmática ha comenzado a centrar sus esfuerzos en la discusión acerca de una nueva teoría de los tipos de delito. En este contexto, ha entrado en una fase de crisis sin aparente solución el tradicional esquema tripartito consistente en distinguir entre delitos de lesión, delitos de peligro concreto y delitos de peligro abstracto, para dar paso a nuevos tipos, entre los que destacan los delitos de aptitud, delitos de acumulación, delitos de preparación y delitos sin bien jurídico[79].

---

77 Entre otros, RALLO LOMBARTE, "De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político*, núm. 100, septiembre-diciembre 2017, pp. 639-669; TERUEL LOZANO, "Derechos fundamentales en la sociedad digital: ¿Hacia una constitución para el ciberespacio?", *Revista chilena de derecho* 46.1 (2019): 301-315.

78 Por ejemplo, en relación a las presunciones algorítmicas que pueden justificar decisiones sobre una sospecha razonable con base en informaciones cruzadas. Al respect, véase, HILDEBRANDT, "Criminal Law and Technology in a Data Driven Society", in: *Oxford Handbook of Criminal Law*, Oxford University Press, 2014, p. 174 y ss.; SOUZA DE MENEZES/AGUSTINA, "Big Data, Inteligencia Artificial y policía predictiva". En Dupuy (dir.) KIEFER (coord.) *Cibercrimen III*, BdF, 2020, pp. 137-181.

79 Véase KUHLEN, "Bienes jurídicos y nuevos tipos de delito". En *Límites al derecho penal: Principios operativos en la fundamentación del castigo*, Robles Planas, R. (ed. española). Atelier, Barcelona, 2013, pp. 225-235.

El ciberespacio presenta, en este sentido, algunas particularidades que merecen especial atención, pues la peligrosidad y escalabilidad de los delitos en los que se utiliza la tecnología desdibujan (y en ocasiones eliminan) la conexión entre los sujetos de carne y hueso y el objeto de protección. Nos hallamos en algunos casos ante delitos sin bien jurídico, esa "categoría sin ulterior desarrollo en la que se reúnen todos los hijos mugrientos de la dogmática penal"[80]. En los delitos sin bien jurídico se podrían llegar a proteger, por ejemplo, meros sentimientos (de seguridad o tranquilidad individual o colectiva)[81]. Para legitimar dicha decisión incriminatoria, se podría intentar satisfacer el dogma del bien jurídico alegando que el bien jurídico es eso mismo, la integridad psíquica colectiva, sin perjuicio de que no existan derechos subjetivos como substrato inmediato o mediato. Se podría también acudir a la doctrina anglosajona del *harm principle*[82], menos exigente en términos dogmáticos. O, en suma, emplear el concepto de bien jurídico, vaciándolo de su núcleo semántico, desde una comprensión puramente metodológica como abreviatura de la idea de fin[83].

Sin duda, la opción político-criminal de incriminar conductas lesivas bajo este nuevo paradigma (protección de realidades virtuales o epidérmicas) plantea un problema de adaptación en los esquemas tradicionales de la dogmática. No pretendo aquí entrar a resolver la cuestión de fondo,

80 KUHLEN, "Bienes jurídicos y nuevos tipos de delito", p. 231.

81 Así, en el delito de stalking no está claro si lo que en realidad se protege no es la libertad o seguridad de la víctima, sino su tranquilidad emocional. Sobre esta cuestión, véase, AGUSTINA/FERNÁNDEZ-CRUZ, "El tipo penal de stalking: una revisión político-criminal tras sus 5 primeros años". En MIRÓ-LLINARES/FUENTES OSORIO (Dirs.), GÓMEZ-BELLVÍS (Coord.), *El Derecho penal ante "lo empírico". Sobre el acercamiento del Derecho penal y la Política Criminal a la realidad empírica*. Madrid: Marcial Pons.

82 FEINBERG*, Offense to others*, Oxford University Press, 1988.

83 KUHLEN, "Bienes jurídicos y nuevos tipos de delito", pp. 230-231.

sumamente compleja y que ha dado lugar a una discusión doctrinal extensa, sino señalar un problema que va a requerir cambios metodológicos y operacionales en el sistema.

En otro lugar me he referido en extenso a las discusiones doctrinales suscitadas en torno a las nuevas formas de incriminación de la pornografía infantil, en concreto, a la pornografía virtual[84] y a la ya referida problemática que plantea la utilización de avatares como cebo para detectar *groomers* y proteger a la comunidad de niños y niñas que utilizan el ciberespacio[85]. Obviamente, los problemas jurídico-penales asociados a las nuevas técnicas de prevención y persecución del delito mediante sistemas de inteligencia artificial constituyen, también, un ámbito novedoso en el que pueden darse algunas tensiones en las categorías dogmáticas y en las garantías procesales que conviene afrontar no solo desde el punto de vista legislativo, sino también desde las estructuras dogmáticas.

En realidad, más allá de si se cuestiona que puedan verse afectados bienes jurídicos en abstracto –lo cual nos parece al menos discutible–, lo que el proyecto Sweetie 2.0 plantea debería enfocarse desde un punto de vista distinto, a saber, la peligrosidad *ex ante* de conductas aparentemente lesivas de bienes jurídicos individuales para proteger la indemnidad sexual de los menores en su conjunto. La discusión del bien jurídico y los modos de ataque al mismo que justificarían la intervención penal ponen encima de la mesa

84 Al respecto, en la Circular 2/2015 de la Fiscalía General del Estado se da cuenta de las novedades introducidas por el Legislador en la reforma del Código Penal de ese mismo año, en la que se incorporan nuevas formas de pornografía infantil (pornografía virtual, pornografía técnica y pseudo-pornografía infantil o *morphing*).

85 AGUSTINA/VARGAS OVALLE, "¿Es necesaria una dogmática de los ciberdelitos? A propósito de la utilización de agentes encubiertos en la lucha contra la explotación sexual de menores en el ciberespacio". En *Derecho penal y persona* (coord. GARCÍA CAVERO/CHINGUEL RIVERA), 2019, *passim*.

la cuestión de los límites materiales de la tentativa relativamente inidónea por inexistencia de objeto. Ese juicio de peligrosidad, al perder la conexión directa con un bien jurídico individualizado se queda a las puertas de la lesión del bien jurídico. De hecho, lo que se lesiona ya no es la indemnidad sexual de una niña, sino los sentimientos de seguridad colectiva de una comunidad que no tolera conductas que coartan de forma grave el disfrute de sus espacios de convivencia[86].

Al final de la discusión nos plantamos, en última instancia, en las necesidades actuales de protección de potenciales víctimas en una sociedad en la que el nivel de tolerancia a asumir cualquier tipo de riesgo con respecto a la infancia se ha reducido de forma considerable. En este punto, la extrema indefensión de potenciales víctimas en el ciberespacio no solo puede legitimar un adelantamiento de las barreras de protección (mediante, por ejemplo, los delitos de *online child grooming*), sino también una ampliación del ámbito de lo punible hasta abarcar algunos casos de inexistencia absoluta de objeto, sin perjuicio de que se lesione un determinado bien jurídico *sui generis* por más abstracto o remoto que pueda parecer a algunos[87].

Junto al problema que plantea *Sweetie*, los delitos cometidos en escenarios virtuales abren nuevos retos que no solo se resuelven con una modificación legislativa, incorporando un nuevo tipo penal. La virtualización del objeto material no es otra cosa que la escisión entre la representación

86 A este respecto, como señala Kuhlen, la postura dominante que sostenía que "no es legítimo crear tipos penales que vayan más allá del peligro abstracto" parece haber reducido de forma significativa su aceptación: véase, KUHLEN, "Bienes jurídicos y nuevos tipos de delito", p. 226.

87 Schünemann se refiere a esta posibilidad y la descarta en casos de inexistencia de un bien jurídico legítimo, como podría ser el tipo penal relativo a la pornografía con animales (SCHÜNEMANN, "Protección de bienes jurídicos, *ultima ratio* y victimodogmática". En *Límites al derecho penal…,* 2012, pp. 82-83).

digital y el substrato personal de la víctima, en tanto que titular del bien jurídico. La cesura entre uno y otro puede ser más o menos radical. Así, por ejemplo, en relación con el fenómeno de los *deepfake*[88] se intuye cómo los casos de suplantación de identidad no solo deben circunscribirse a la sustitución de la persona real en el tráfico jurídico o económico, sino que la mera utilización de la propia imagen en el ciberespacio puede causar un daño *sui generis*, aparente y tal vez momentáneo, aunque no por ello menos significativo, en la reputación de la víctima. La lesión virtual o efímera del bien jurídico mediante el uso de una imagen distorsionada y falsa se sustenta en un concepto volátil, ciertamente vaporoso, de honor e integridad moral, basado en la identificación de una imagen distorsionada de la víctima con el sujeto real.

Del mismo modo, las estratagemas mediante la utilización de scam o ransomeware pueden impactar en potenciales víctimas que, por diversos motivos, no estén en disposición de *morder el anzuelo* o no tengan nada que perder. O los hackers pueden intentar entrar sin éxito en un sistema que se halle perfectamente blindado… o que sea inexistente (por tratarse de un *honeypot*)[89]. En tales casos no podría objetarse, a mi juicio, que la tentativa no es punible por inexistencia de objeto. En el ciberespacio los intentos de cometer un delito con éxito se basan en una lógica distinta: (1) en primer lugar, en términos de escalabilidad, los frutos o efectos del delito

88 Véase, KIRCHENGAST, "Deepfakes and image manipulation: criminalisation and control", *Information & Communications Technology Law* 29.3 (2020), p. 1: "Deepfakes are a form of human image synthesis where an existing picture or image is superimposed into a video to change the identity of those depicted in the video. The technology relies on machine learning or artificial intelligence to map an existing image, usually a photo of a person's face, to transfer that image to an existing video image".

89 *Honeypots* son sistemas informáticos diseñados expresamente para ser atacados y así permitir a los que pretenden defenderse aprender sobre métodos de ataque (ROWE/CUSTY/DUONG, "Defending cyberspace with fake honeypots", *Journal of Computers* 2, no. 2 (2007): 25-36).

poseen un alcance ilimitado, abriéndose el curso de acción a múltiples destinatarios; (2) en segundo lugar, en términos de optimización de recursos, los autores logran ese efecto multiplicador con una sola acción y sin un esfuerzo adicional significativo; y (3) por último, en el conjunto de los medios de ataque los intentos fallidos revisten una importancia menor o insignificante: solo un porcentaje de incautos sucumbirá, mientras que el resto de mortales habrá reaccionado de forma adecuada a un riesgo típico que, desde la perspectiva del hombre medio, cabría considerar que llegaría al umbral del engaño bastante.

En el mundo de las apariencias del ciberespacio, los menores de edad pueden ser avatares que se empleen como cebo o adultos disfrazados de menores; los sitios web pueden ser *honeypots*; los destinatarios de un listado de correos pueden estar inactivos desde hace mucho tiempo; quien dice ser quien es, puede ser que no lo sea; o quien aparenta capacidad adquisitiva o poder de disposición, pueda estar absolutamente incapacitado (por ejemplo, para lograr con éxito una estafa del CEO). Sin embargo, la peligrosidad residual que se desprende de los intentos aleatorios o lanzados al azar no dejan de afectar a la seguridad global del ciberespacio, sin perjuicio de que, en un análisis pormenorizado (y siempre ex post facto), veamos que, en realidad, eran irrelevantes por inexistencia de objeto. Que no haya niña de carne y hueso o que se trate de un adulto en lugar de un menor es, a mi juicio, una cuestión indiferente a los efectos de valorar la peligrosidad ex ante.

Todas estas consideraciones nos conducirían a justificar una modulación en el concepto de bien jurídico y en la dogmática de la tentativa cuando el objeto de ataque es virtual. Para acercarse a los nuevos problemas con un criterio adecuado de dañosidad o peligrosidad, en ese sentido, sería necesario acudir al *hombre medio* y a la teoría de la conmoción en un mundo en el que la apariencia posee un significado distinto. Enlazando con lo apuntado sobre la modulación del concepto de acción y de la fenomenología del iter

criminis, en el ciberespacio las acciones no físicas en que consisten los intentos penalmente relevantes, responden a una lógica distinta. Lo que se intenta en Internet se acerca a los meros pensamientos porque en el ciberespacio se puede intentar todo sin aparentes consecuencias. La aparente *levedad del ser* de lo virtual nos debería llevar a resaltar mejor que esos intentos sin calibrar quién está detrás de cada destinatario virtual no dejan de revestir una peligrosidad intolerable. Con bien jurídico, sin bien jurídico o con un *tertium genus*.

5.3. Imputación objetiva, autoría y participación y otras cuestiones

Finalmente, apuntaré muy sucintamente otras cuestiones problemáticas para la reflexión dogmática en relación con el ciberdelito, que se derivan de algún modo de las modulaciones apuntadas (sobre los conceptos de acción y bien jurídico).

En efecto, a consecuencia de lo que se acaba de señalar, la relación de causalidad e imputación objetiva en el ciberespacio plantea algunas especificidades. Los efectos y la rapidez con que se difunde la información en las redes sociales, por ejemplo, plantea problemas nuevos en relación con la criminalización de la creación y difusión de *fake news*[90]. El ciberespacio es, en este sentido, un *contexto panicógeno*, es decir, un terreno propicio para generar una sensación social de inseguridad y miedo conducente al pánico u ofuscación colectiva que, de forma descontrolada, puede abocar a un número considerable de personas a adoptar decisiones perjudiciales para sí mismas y/o para una pluralidad indeterminada de personas. Ese pánico u ofuscación colectiva podría, eventualmente, explicar, por ejemplo: (i) una frenética caída en el mercado bursátil o una retirada masiva de depósitos bancarios, provocando ingentes pérdidas económicas a todo

90 Véase, GUERINI, *Fake news e diritto penale*, Giappichelli, Torino, 2020.

un país; (ii) un contagio masivo exponencial de personas que, de forma ineludible, colapsara las unidades de cuidados intensivos traduciéndose en muertes por escasez de recursos disponibles; o (iii) una pérdida súbita de confianza por parte de un número significativo de ciudadanos en un candidato electoral ante la inminencia del día de la votación.

Muchas son las cuestiones que dificultan el análisis de la relación de imputación objetiva. Entre los posibles factores desencadenantes de un estado de pánico colectivo debería sobresalir con una significación y peso determinante la irrupción de una noticia falsa (fakenews) o bulo. No obstante, no cabe duda de que el poder o eficacia de unas fakenews solo se explica en el contexto de una atmósfera colectiva hipersensibilizada frente a un determinado peligro. Ante la posible responsabilidad penal por las consecuencias derivadas de una noticia falsa surgen tres cuestiones:

(1) No toda noticia falsa es igualmente dañina en términos de previsibilidad, ni responde siempre a una intencionalidad determinada. En ocasiones, puede originarse en una intolerable equivocación de diagnóstico o impericia manifiesta que revelaría un error en la representación del riesgo que podría excluir el dolo eventual. Sería, por tanto, imprescindible describir una taxonomía de noticias falsas penalmente relevantes.

(2) La inmediatez y magnitud de los efectos desencadenantes de un eventual resultado no es explicable si no se atiende a un cambio de escenario en las reglas de imputación objetiva. Esa previsibilidad en el ciberespacio es aleatoria, cuando no caprichosa o impredecible. Solo aquellos mensajes o noticias falsas que revistan peligrosidad ex ante de acuerdo con las reglas del ciberespacio y que se concreten en un peligro concreto, podrían justificar una imputación del resultado o del riesgo generado.

(3) Difícilmente las figuras delictivas clásicas podrían cubrir la imputación de los resultados lesivos finalmente

producidos. Los tipos genéricos de homicidio o estafa teóricamente serían idóneos, por ejemplo, para subsumir en ellos decisiones ruinosas en lo económico o muertes aparentemente causadas por las propias víctimas de la desinformación. Con todo, la distancia o, mejor dicho, la concatenación de factores intermedios, dificulta enormemente la prueba del nexo de imputación objetiva. Y, sobre todo, la ausencia de resultados por intervenciones de terceros que hayan contrarrestado el efecto inicial, arroja poderosas razones de conveniencia para crear tipos específicos de peligro abstracto-concreto.

Asimismo, como es sabido, desde el surgimiento de la perspectiva victimológica los delitos son ya para siempre eventos o acontecimientos en los que concurren dos comportamientos bidireccionales[91]. En la víctima se puede requerir, para algunos delitos, que consienta o actúe engañada y bajo error. Las interacciones en el ciberespacio pueden ser asincrónicas[92] y en ellas la representación de la realidad puede sufrir, con mayor facilidad, algunas distorsiones, también en relación a la persona (su edad, experiencia e incluso su propia identidad).

Teniendo en cuenta las distorsiones cognitivas y volitivas ya apuntadas, todos estos elementos pueden conllevar interesantes y complejas interferencias victimo-dogmáticas. Junto a los problemas ya referidos en relación al delito de estafa, en el delito de *grooming* se junta el hambre (del *groomer*) con las ganas de comer (de la víctima, pues con frecuencia no actúa bajo error aparente)[93]. En ambos casos las percepciones y condicionantes psicológicos que derivan del entorno

91 Véase, al respecto, BERGELSON, *Victims' Rights and Victims' Wrongs*, 2009, *passim*. He tratado en extenso sobre este enfoque aplicado al ciberespacio en AGUSTINA, "Cibercriminalidad y perspectiva victimológica…", p. 153 y ss.

92 SULER, "The Online Disinhibition Effect", *Cyberpsychology & Behavior*, Volume 7, Number 3, pp. 322-323.

93 WOLAK/FINKELHOR/MITCHELL, Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, 35 (2004), 424.e11– 424.e20.

tecnológico deberían tenerse en cuenta. No es lo mismo interactuar offline que hacerlo online, como ya se ha señalado. Más allá del efecto desinhibidor, las situaciones de error y los déficits de autocontrol que son inherentes al ciberespacio deberían pesar en la valoración de los requisitos necesarios para imputar responsabilidad o para exonerar de ella a quien no ha actuado con la información y libertad necesarias. Piénsese, por ejemplo, en el consentimiento libre del menor de 16 años que mantiene una relación sexual online con un mayor de edad, próximo en edad y madurez (art. 183 quáter). ¿Al apreciarse la libertad del consentimiento debería valorarse con un mayor estándar si fue prestado online? A mi juicio, sí, en tanto que el grado de libertad en el ciberespacio, con todos sus condicionamientos, es sensiblemente menor.

Otro ámbito de cuestiones sumamente importantes hace referencia a los criterios de autoría y participación en el marco de interacciones entre humanos y ordenadores, posean o no inteligencia artificial.

Por un lado, no plantearía problema alguno la utilización de la tecnología como forma de controlar otros entes programados, siendo una forma intermedia o mixta dirigida a lesionar bienes de terceros. Así, por ejemplo, la intervención articulada de un ejército de *bots* para perpetrar un ataque de denegación de servicios no dejaría de considerarse una forma de autoría directa. En cambio, se pueden dar estructuras de autoría mediata cuando esos instrumentos, aun gozando de relativa autonomía, posean información limitada acerca del alcance de su actuación. Por ejemplo, la publicación del teléfono móvil de la víctima en un anuncio de relaciones generaría un aluvión de contactos indeseados orquestados por el autor de un delito de stalking. Lo mismo podría suceder con el autor de una noticia falsa sobre la víctima que desencadena una reacción viral contra ella, cristalizando incluso en discurso de odio.

El problema se puede complicar todavía más cuando al ciberespacio como canal de una diversidad de medios de comunicación, se le suma un conjunto de entes ejecutores o decisores, con mayor o menor autonomía (siempre programada en última instancia). Obviamente, ante el auxilio o colaboración de inteligencias artificiales, desde el derecho privado deberá delimitarse bien quién responde en caso de fallo técnico: ¿el usuario, el diseñador, programador, quien gestiona el servicio de atención al usuario o el propio artefacto? Y, en sede penal, habrá que dilucidar qué grado de diligencia debida puede exonerar al (pobre) ser humano que tenga que estar pendiente de un número ilimitado de cosas inteligentes a su alrededor[94].

En ese complejo entramado el deber de evitar *outputs* lesivos requiere de una cierta reflexión dogmática. Entramos, desde una perspectiva del *compliance*, en una amalgama de información y decisiones en la que la trazabilidad es clave. La novedad del problema es que a la hora de imputar responsabilidad nos podemos llegar a encontrar con entes gobernados por IoT (*Internet of Things*), alimentados por un flujo de datos de origen conocido o ignoto, a los que se pueden sumar algoritmos (semi-transparentes o totalmente opacos) con forma de inteligencias artificiales o robots de diverso alcance. Todo ello puede oscurecer el juicio de imputación y generar espacios de concurrencia de comportamientos imprudentes.

No me refiero a la cuestión de si, en un futuro, se planteará la responsabilidad penal de los robots. La división del trabajo y delegación de funciones entre seres humanos e inteligencias artificiales no ha hecho más que comenzar. Los roles asignados a cada interviniente y los límites con que deba reformularse el principio de confianza deberían clarificarse.

94 Sobre tales cuestiones, véase el interesante análisis de HILDEBRANDT, "Ambient intelligence, criminal liability and democracy." Criminal Law and Philosophy 2.2 (2008): 163-180.

Las tres leyes de la robótica de Asimov[95] eran, desde esta perspectiva, simplistas.

Finalmente, los problemas que se acaban de sugerir nos conducen al concepto de persona y a la redefinición de sus atributos en un mundo con realidad virtual, aumentada o biónica. Aquí habría que distinguir tres cuestiones: (1) la persona como sujeto de atribución (de conductas realizadas mediante o sobre entes subordinados o prolongaciones de la persona), (2) como sujeto de imputación (en relación a si es posible concebir otros entes no humanos como persona responsable penalmente) y (3) los condicionantes y características de la persona mediada por la tecnología.

Así, como sujeto de atribución me refiero a la cuestión de hasta qué punto o con qué criterios lo protagonizado o sufrido por un avatar se puede reconducir a una persona humana. En cambio, como sujeto de imputación cabe plantearse si en el futuro a un robot, desgajado del todo de la persona humana que lo programó y puso en funcionamiento, se le reconoce (por una decisión valorativa del sistema) el estatuto de sujeto penalmente responsable. No dejaría de ser una *fictio iuris*, como sucede con las personas jurídicas. La autonomía, como la libertad de voluntad, es una cuestión de grado en el ser humano; *mutatis mutandis*, a partir del proceso de autoaprendizaje y *machine learning* se podría entender que puede concurrir, en algunos casos, una cierta derivación autónoma "consciente", aunque los robots no se podrían apartar de las normas básicas. La cuestión clave, a mi juicio, no será si el ente robotizado revestirá algún día plena o suficiente autonomía, entre otras cosas porque con las personas jurídicas la respuesta es siempre negativa: estas nunca gozan de ningún tipo de autonomía *per se*, sino a través de sus órganos, representantes e incluso de sus empleados de nivel inferior no

95 CLARKE, "Asimov's laws of robotics: Implications for information technology", *Machine ethics* (2011): 254-84.

debidamente supervisados. Por limitaciones de espacio, dejaré esta segunda cuestión para futuros trabajos[96].

En cuanto a la persona como sujeto de atribución debemos interrogarnos acerca de si existe una plena identidad entre yo-real y yo-digital. Desde el funcionalismo y la teoría del rol, el concepto de persona se refiere a la representación del individuo hacia el exterior que permite reducir la complejidad de las interacciones sociales y centrarse en un conjunto de expectativas sociales derivadas de esa máscara que caracteriza y se impone al sujeto[97]. Dentro de ese esquema, un sujeto puede, al conformar su persona, asumir distintos roles y será en función de las particularidades de cada relación social como se definirá su posición jurídica (derivada de cada rol).

En el ciberespacio, la persona puede asumir tantas máscaras como desee, desvinculadas unas de otras. Esa reducción de la complejidad se construye sobre pautas de orientación ciertamente confusas. El yo-real (la persona) se puede convertir y desdoblar en identidades digitales absolutamente alejadas del nivel de competencia o de los atributos reales del sujeto. La representación del yo es, pues, ficticia y deslavazada porque no atiende a reglas predefinidas. Todo vale.

En ese contexto, una persona se puede dividir en múltiples usuarios, entendiéndose por usuario aquel sujeto funcional que utiliza su identidad digital (y la de sus dispositivos), mediante una conexión virtual a los sistemas que le

96 Sobre esta cuestión, véase POSADA MAYA, "La responsabilidad penal de los agentes de inteligencia artificial: entre la ficción y una realidad que se aproxima". En PORTILLA CONTRERAS/VELÁSQUEZ VELÁSQUEZ/POMARES CINTAS/FUENTES OSORIO, *Un juez para la democracia: libro homenaje a Perfecto Andrés Ibáñez*, Dykinson, Madrid, 2019.

97 JAKOBS, *Sociedad, norma y persona…,* 1996; PIÑA ROCHEFORT, *Rol social y sistema de imputación: una aproximación sociológica a la función del derecho penal*. JM Bosch Editor, 2005.

otorgan privilegios informáticos y jurídicos, para interactuar en el ciberespacio (como realidad simulada), con diversos fines, pudiendo llevar a cabo determinados propósitos, algunos penalmente relevantes[98].

Llevando las cosas al extremo, ¿qué criterios de asignación en términos de autoría se deberían emplear para, por ejemplo, un avatar que interactúe y llegue a cometer delitos virtuales[99] en un mundo completamente simulado? ¿Se debe atribuir a la persona, como sujeto activo o pasivo, los mensajes transmitidos mediante realidad virtual? En ese sentido, ¿cómo deberíamos valorar la representación simulada de imágenes íntimas como si fueran reales a efectos del delito difusión inconsentida de imágenes íntimas? Y respecto de los delitos cometidos en un mundo completamente virtual, ¿cuándo serían solo un juego y cuándo comportarían consecuencias con impacto en la realidad física? La realidad aumentada y la interconexión de los mundos online y offline pueden sorprendernos, como a Wade Owen Watts en la producción de Spielberg *Ready Player One* (2018). Dicho de otro modo, ¿qué distingue, a efectos penales, un *hecho real* de un *hecho virtual* cometido sobre *personas totalmente virtuales*? La separación entre ambos mundos empieza a ser borrosa, si bien lo que distingue a un juego de la vida real es precisamente que la finalidad del primero (la pura diversión) evita la asunción de responsabilidad más allá de las reglas y marco de sentido de ese juego.

Finalmente, por último, y no por ello menos importante, en cuanto a los condicionantes y características de la persona que actúa en el ciberespacio, cabría plantearse si po-

98 MEEK NEIRA, *Delito informático y cadena de custodia*, 2013, pp. 39-40; POSADA MAYA, El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual, *Nuevo Foro Penal*, 13(88) (2017), pp. 88-89.

99 Por ejemplo, en escenarios como las comunidades virtuales en *Second Life*. Véase, BRENNER, "Is There Such a Thing as 'Virtual Crime'?", *California Criminal Law Review*, 4(1) (2001).

drían dar lugar a la creación de circunstancias atenuantes o agravantes de diversa naturaleza.

Respecto de las primeras, las situaciones de error y consentimiento viciado en la víctima, por ejemplo, podrían ser factores que llegaran a atenuar el juicio de reproche sobre el autor. Piénsese, por ejemplo, en lo referido *supra* respecto del octogenario acusado de difundir pornografía infantil que desconocía que sus archivos estaban siendo utilizados por terceros (ignorando que el programa P2P permitía esa posibilidad). O en el sujeto que se fía de la fotografía manipulada del perfil de una menor, mostrando rasgos inequívocos de adulto.

En cuanto a las circunstancias agravantes, nos hemos referido en líneas anteriores a la posibilidad de que el legislador incorpore en los delitos tradicionales subtipos que recojan lo específico del injusto cometido a través de las TIC, con la consiguiente agravación en la pena del tipo básico. No obstante, también se podría acudir a una regla general en algunos casos, mediante la creación de una circunstancia agravante específica[100] o incluso subsumir la utilización de las TIC en el abuso de superioridad, como tipología de disfraz o de lugar cuyas circunstancias "debiliten la defensa del ofendido o faciliten la impunidad" (art. 22.2º CP). Esta solución, sin duda, podría colmar ese plus de desvalor inherente a las conductas perpetradas a través de las TIC. En ese sentido, el ciberespacio sería considerado, como ya hemos señalado, un lugar criminógeno en el que las condiciones de anonimato podrían justificar una agravación punitiva derivada de la referida peligrosidad.

A tales efectos, convendría introducir una nueva circunstancia modificativa en el Código penal español en la que

100 Como en Colombia: art. 58.17ª CP (introducido por la Ley 1273 de 2009). Véase, al respecto, POSADA MAYA, *Los cibercrímenes: un nuevo paradigma de cibercriminalidad*, pp. 102-103.

se incluyeran las diferentes razones por las que un ciberdelito puede resultar un hecho de mayor gravedad con respecto a la misma conducta realizada en el espacio físico. Se podría, así, incorporar al artículo 22 una 9º circunstancia, una nueva agravante por razón de los medios tecnológicos empleados que, por su naturaleza, faciliten, aumenten o intensifiquen la perpetración o los efectos de cualquier conducta delictiva. o dificulten la identificación del autor o su persecución.

6. Conclusiones

El objetivo del presente trabajo se ha limitado a plantear la conveniencia (o no) de adaptar, mediante un enfoque específico, el análisis dogmático ante los delitos cometidos a través de la tecnología. Para responder a esta cuestión se ha utilizado un método de análisis multidisciplinar. Partiendo de un enfoque criminológico, se ha tratado de argumentar cómo las mutaciones experimentadas en la era digital acaban impactando de forma significativa en las categorías dogmáticas, tensionando sus costuras. La extensión de la primera parte ha obedecido a la necesaria fundamentación de una forma algo heterodoxa de articular un discurso dogmático, apoyado en consideraciones alejadas en parte de una perspectiva racional centrada en lo jurídico. En todo caso, no se ha pretendido proyectar la discusión en problemas concretos, profundizando en exceso en cuestiones específicas que, a lo largo del texto, han servido como meros ejemplos de la cuestión de partida. Los problemas más específicos que se han referido merecerán sin duda un enfoque más incisivo en futuros trabajos.

A lo largo del texto se ha visto cómo con la intensificación de la transformación digital, las actividades cotidianas de las personas, así como la forma de interaccionar unos con otros y con el mundo, han resultado significativamente alteradas. Podría decirse que, en este nuevo contexto, el modo de

obrar (*modus operandi* en sentido amplio) responde a unas características distintas, habiéndose alterado también la forma de cometer delitos. Este cambio plantea una clave explicativa nueva en la dinámica comisiva del delito, de cualquier delito. Y, como he tratado de analizar en las líneas precedentes, tales cambios han impactado también de algún modo en las tradicionales estructuras de imputación de responsabilidad. Más aún, a consecuencia de tales transformaciones contextuales, el ser humano ha visto moduladas sus facultades cognitivas y volitivas. Así las cosas, condicionado por una alteración de tanto calado en su *modus vivendi*, e incluso su *modus essendi*, se ha concluido que, en efecto, las categorías de la teoría del delito requieren de una cierta adaptación si se pretende ajustar el sistema a la nueva realidad existencial.

Con el objetivo de clarificar los distintos aportes, he llevado a cabo una revisión del concepto de ciberdelito y su naturaleza desde una perspectiva funcional. Pese a los esfuerzos definicionales, he argumentado que el concepto de ciberdelito, desde las cuatro perspectivas analizadas (criminológica, penal, dogmática y procesal), tiene *fecha de caducidad*: responde a una necesidad *aquí y ahora* de afrontar algo nuevo, por lo que, una vez se reajuste y normalice la respuesta del sistema, es esperable que vaya perdiendo su fuerza expresiva. En un estadio próximo no será necesario (sino que será superfluo o extraño) distinguir entre lo físico y lo virtual como partes de una misma realidad. Lo decisivo es, pues, la adaptación del sistema a un nuevo método de análisis que comprenda lo distintivo en el modo de cometer *hoy* cualquier delito. Sin perjuicio del nombre o de la cuestión clasificatoria, atender a la dinámica comisiva de los ciberdelitos se revela sobre todo muy útil, ciertamente, desde el punto de vista criminológico, a fin de enfocar de modo particular las estrategias de prevención para cada tipología delictiva en un contexto novedoso. Pero, como se ha dicho, su utilidad o conveniencia va más allá de lo criminológico o de las cuestiones meramente procesales.

En esta tesitura, la necesidad de una teoría adaptada al nuevo entorno social para afrontar en última instancia el juicio de subsunción pasa por un nuevo entendimiento de algunos conceptos tradicionales de la teoría del delito.

A lo largo de mi hilo discursivo se han tratado de sentar las bases para una reflexión dogmática imprescindible (que, en todo caso, convendrá desarrollar) para mejorar la respuesta y los instrumentos concretos frente a un nuevo paradigma de criminalidad. Así, en concreto, más allá de (1) una reconceptualización del concepto de acción, se ha puesto encima de la mesa la necesidad de (2) repensar las bases ontológicas sobre las que se construye el instituto de la prescripción del delito y (3) la teoría de concursos en un escenario de contracción espacio-temporal. Asimismo, se ha visto necesario reformular (4) el mismo concepto de bien jurídico, con todas las implicaciones que ello puede comportar, por ejemplo, en (5) la dogmática de la tentativa. La lesión o puesta en peligro de un bien jurídico virtualizado (cuya existencia es en ocasiones mera potencia), en una sociedad en la que el delito es más que nunca una *comunicación de sentido* sin base necesariamente física, puede realizarse en supuestos no solo de lejanía espacial entre ofensor y víctima, sino en casos de conexión remota o indirecta entre los sujetos representados y la realidad representada. La teoría de la conmoción podría servir de justificación, en ese sentido, a una necesidad de reacción ante tentativas sin objeto real (inexistencia de objeto) o delitos sin bien jurídico.

También se han apuntado (6) algunas cuestiones sobre cómo el entorno tecnológico incide en el análisis de los problemas de autoría y participación, así como otras relacionadas con el concepto de persona, surgidas de la interacción entre seres humanos cuando intervienen en la ejecución de los hechos entes supuestamente con cierta autonomía funcional. Finalmente, a la luz de las modulaciones en las facultades cognitivas y volitivas en el ciberespacio, se han propuesto

algunas reflexiones en sede de (7) imputación objetiva y desde la perspectiva victimo-dogmática (a tenor de los déficits en la comprensión de las interacciones y de las situaciones de error o vicios en el consentimiento producidos) y (8) algunas consideraciones sobre las circunstancias atenuantes y agravantes que convendría analizar en profundidad, sugiriendo la introducción de una nueva circunstancia agravante por razón de los medios tecnológicos empleados en el delito.

Con todo, los límites de mi propuesta de revisión son evidentes. Este trabajo solo ha apuntado numerosas cuestiones que, sin llegar a resolverlas, enfatizan una necesidad de reajuste en el enfoque dogmático. Sin la revisión de ese sustrato dogmático, las reformas penales e incluso la labor jurisprudencial se encontrarán con inconsistencias, lagunas y falta de entendimiento de los fenómenos delictivos a los que necesita hacer frente. La discusión acaba de comenzar y, de buen seguro, la pretensión de *volcar* todo el bagaje de la teoría del delito a las *nuevas* formas de criminalidad redundará en una dogmática revitalizada. Solo una dogmática que se preocupe por lo nuevo será capaz de justificar su función esencial: preservar el sistema de justicia penal de los vaivenes del legislador y de la inseguridad de una jurisprudencia huérfana de la necesaria reflexión conceptual.

Con todo, a la vista de lo expuesto y dada la heterogeneidad y transversalidad que caracterizan los problemas que suscitan los ciberdelitos (toda infracción penal puede perpetrarse a través de las TIC), no se justifica la creación de una dogmática del ciberdelito, con autonomía y fines propios, similares a la dogmática de las distintas estructuras comisivas, que sí han merecido una atención y tratamiento doctrinal diferenciado (como en el caso del tipo de omisión, el tipo imprudente o los tipos de imperfecta realización, por ejemplo). La comisión de un hecho delictivo a través de las TIC no reviste, a estos efectos, de la necesaria singularidad como para merecer un estudio dogmático sistemáticamente

organizado, sin perjuicio de que, como se ha señalado, existan importantes cuestiones dogmáticas que, en el contexto tecnológico, requieran de adecuadas reflexiones doctrinales que se traduzcan en reajustes, en algunos casos sin duda relevantes. En futuros trabajos será necesario categorizar en detalle los problemas aquí apuntados y establecer criterios generalizables o definitorios que, por el objeto de estas líneas, excederían el propósito de partida.

Bibliografía

ABOSO (2017). *Derecho penal cibernético*. BdeF, Buenos Aires-Montevideo.

AGUSTINA (2009). "La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual". *International e-journal of criminal sciences*, (3), pp. 4-31.

AGUSTINA (2014). "Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización". *Cuadernos de política criminal*, 114(III), pp. 143-178.

AGUSTINA/MONTIEL/GÁMEZ (2020). *Cibercriminología y victimización online*. Editorial Síntesis, Madrid.

AGUSTINA (2010). "¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el sexting". *Revista Electrónica de Ciencia Penal y Criminología*, 12(11), pp. 1-44.

AGUSTINA/VARGAS OVALLE (2019). "¿Es necesaria una dogmática de los ciberdelitos? A propósito de la utilización de agentes encubiertos en la lucha contra la explotación sexual de menores en el ciberespacio". En *Derecho penal y persona* (coord. García Cavero y Chinguel Rivera). Ideas Solución Editorial, Lima, Perú, pp. 609-644.

AGUSTINA/FERNÁNDEZ-CRUZ (*in press*). "El tipo penal de stalking: una revisión político-criminal tras sus

5 primeros años". En F. Miró-Llinares/J.L. Fuentes Osorio (Dirs.), A.B. Gómez-Bellvís (Coord.), *El Derecho penal ante "lo empírico". Sobre el acercamiento del Derecho penal y la Política Criminal a la realidad empírica*. Marcial Pons, Madrid.

ALTER (2017). *Irresistible: The rise of addictive technology and the business of keeping us hooked*. Penguin.

BERGELSON (2009). *Victims' Rights and Victims' Wrongs. Comparative Liability in Criminal Law*. Standford University Press.

BOTTOMS (2008). The relationship between theory and empirical observations in criminology, R.D. King/E. Wingcup, *Doing research on crime and justice*, Oxford University Press, pp. 75-116.

BRENNER (2001), Is There Such a Thing as 'Virtual Crime'?, *California Criminal Law Review*, 4(1).

CANEPPELE/AEBI (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, 13(1), 66-79. https://doi.org/10.1093/police/pax055

CLARKE (2011). Asimov's laws of robotics: Implications for information technology, *Machine ethics* (2011): 254-84. https://doi.org/10.4324/9781003074991-4

CLOUGH (2015). *Principles of cybercrime*. Cambridge University Press.

COCA VILA (2017). "Coches autopilotados en situaciones de necesidad: una aproximación desde la teoría de la justificación penal", *Cuadernos de Política Criminal*, núm. 122, II, Época II, septiembre 2017, pp. 235-275.

COHEN/FELSON (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608. https://doi.org/10.2307/2094589

DÍEZ RIPOLLÉS (2003). *La racionalidad de las leyes penales*. Trotta, Madrid.

ECK (1997). Do premises liability suits promote business crime prevention? In Felson, M., Clarke, R.V. (eds.), *Business and Crime Prevention*, New York, 125-150.

FELSON (1997). Technology, Business and Crime. In Felson, M., Clarke, R.V. (eds.), *Business and Crime Prevention*, Criminal Justice Press, New York, pp. 81–96.

GARCÍA AMADO (2003). "Anatomía de un imposible. La imagen jurisprudencial del policía". En C. da Agra, J. L. Domínguez, J. A. García Amado, P. Hebberecht y A. Recasens (eds.), *La seguridad en la sociedad del riesgo*, Madrid, Atelier, pp. 181-200.

GILLESPIE (2015). *Cybercrime: key issues and debates*. Routledge. https://doi.org/10.4324/9781315884202

GOODMAN, M. (2015). *Los delitos del futuro*. Ariel, Barcelona.

GOTTFREDSON/HIRSCHI. *A general theory of crime*. Stanford University Press, 1990.

GRABOSKY. "Virtual criminality: Old wine in new bottles?", *Social & Legal Studies*, 10(2) 2001, 243-249.

HAN (2014). *Psicopolítica*. Herder, Barcelona.

HERNÁNDEZ DÍEZ (2010). "Aproximación a un concepto de Derecho penal informático". En De la Cuesta Arzamendi/De la Mata Barranco, *Derecho penal informático*, p. 31 y ss.

HINDELANG/GOTTFREDSON/GAROFALO (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

HILDEBRANDT (2008). Ambient intelligence, criminal liability and democracy, *Criminal Law and Philosophy* 2.2 (2008): 163-180.

HILDEBRANDT (2014). Criminal Law and Technology in a Data Driven Society, in: *Oxford Handbook of Criminal Law*, Oxford University Press, 2014.

HOLT/BOSSLER/SEIGFRIED-SPELLAR (2017). *Cybercrime and digital forensics: An introduction*. Routledge.

JAKOBS (1996). *Sociedad, norma y persona en una teoría de un Derecho penal funcional*. Civitas, Madrid.

JESCHECK/WEIGEND (2002). *Tratado de Derecho penal* (trad. Olmedo Cardenete). Comares, Madrid.

KATYAL (2002). *Digital architecture as crime control*. Yale Law Journal, 112, 2261. https://doi.org/10.2307/3657476

KIRCHENGAST (2020). "Deepfakes and image manipulation: criminalisation and control." *Information & Communications Technology Law* 29.3 (2020): 308-323. https://doi.org/10.1080/13600834.2020.1794615

KRÄMER (2008). *Medium, Bote, Übertragung: Kleine Metaphysik der Medialität*, Frankfurt a. M.: Suhrkamp.

KUHLEN (2013). "Bienes jurídicos y nuevos tipos de delito". En *Límites al derecho penal: Principios operativos en la fundamentación del castigo*, Robles Planas, R. (ed. española). Atelier, Barcelona, pp. 225-235.

KURZWEIL (2005). *The singularity is near: When humans transcend biology*. Penguin.

LARRAURI (2015). *Introducción a la Criminología y al sistema penal*, Trotta, Madrid.

LAVORGNA (2020). *Cybercrimes*, MacMillan, Red Globe.

LESSIG (2006). *Code 2.0*, Basic Books.

MATA Y MARTÍN (2003). "Criminalidad informática: una introducción al cibercrimen", *Actualidad penal* 37 (2003).

MAYER LUX (2017). "El bien jurídico protegido en los delitos informáticos", *Revista chilena de derecho*, 44(1), 261-285. https://doi.org/10.4067/s0718-34372017000100011

MEEK NEIRA (2013). *Delito informático y cadena de custodia*. Universidad Sergio Arboleda, Bogotá, 2013.

MIRÓ (2011). "La oportunidad criminal en el ciberespacio", *Revista Electrónica de Ciencia Penal y Criminología* 7 (2011): 1-07.

MIRÓ (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons, Madrid.

MIRÓ (2016). "La cibercriminalidad 2.0: falacias y realidades", En: *Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal*, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda.

MIRÓ/MONEVA (2020). Environmental Criminology and Cybercrime: Shifting Focus from the Wine to the Bottles. In: *The PalgraveHandbook of International Cybercrime and Cyberdeviance*, 2020, pp. 491-511.

MONTIEL/AGUSTINA (2019). "Retos educativos ante los riesgos emergentes en el ciberespacio", *Revista Española de Pedagogía*, 77(273), pp. 277-294. https://doi.org/10.22550/rep77-2-2019-03

MONTORO (2019). "Pedodolls y pedofilia: límites y evidencias en torno a la utilización de muñecas sexuales con rasgos infantiles", *Revista Española de Investigación Criminológica* 17 (2019), pp. 1-25. https://doi.org/10.46381/reic.v17i0.251

MORALES PRATS/GARCÍA ALBERO (2011). "Delitos contra la libertad e indemnidad sexuales". En Quintero Olivares (dir.) y Morales Prats (coord.), *Comentarios a la parte especial del derecho penal*, Thomson Reuters Aranzadi, Navarra, pp. 1269-1405.

MUSK (2019). "An integrated brain-machine interface platform with thousands of channels", *Journal of medical Internet research* 21.10 (2019): e16194. https://doi.org/10.2196/16194

OGBURN (1964). *On culture and social change: selected papers*. Chicago: University of Chicago Press.

OST (2009). *Child pornography and sexual grooming: Legal and societal responses*. Cambridge University Press. https://doi.org/10.1017/CBO9780511730047

PIÑA ROCHEFORT (2005). *Rol social y sistema de imputación: una aproximación sociológica a la función del derecho penal*. JM Bosch Editor, Barcelona.

PEASE (2003). Crime futures and foresight: Challenging criminal behaviour in the information age. In *Crime and the Internet* (pp. 30-40). Routledge. https://doi.org/10.4324/9780203164501_chapter_2

POSADA MAYA (2017). *Los cibercrímenes: un nuevo paradigma de cibercriminalidad*. Universidad de los Andes, Colombia, 2017.

POSADA MAYA (2017). "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual". *Nuevo Foro Penal*, 13(88), pp. 72-112.

PRATT/CULLEN (2000), The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis, *Criminology*, 38, 931-964.

RALLO LOMBARTE (2017). "De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político*, núm. 100, septiembre-diciembre 2017, pp. 639-669.

ROMEO CASABONA (2006). "De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal". En *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Carlos María Romeo Casabona (coord.), Estudios de derecho penal y criminología 78. Comares, Madrid, pp. 1-43.

SCHERMER *et al.* (2016). *Legal Aspects of Sweetie 2.0*. Leiden University, Faculty of Law & Tilburg University, Faculty of Law.

SCHÜNEMANN (2012). "Protección de bienes jurídicos, ultima ratio y victimodogmática". En *Límites al derecho penal: Principios operativos en la fundamentación del castigo*, Robles Planas, R. (ed. española). Atelier, Barcelona, pp. 82-83.

SILVA SÁNCHEZ (2011). *La expansión del derecho penal. Aspectos de la política criminal en las sociedades*

postindustriales (3ª ed.), BdeF, Buenos Aires-Montevideo, 2011.

SILVA SÁNCHEZ (2010). *Aproximación al Derecho penal contemporáneo* (2ª ed.), BdeF, Montevideo-Buenos Aires.

SILVA SÁNCHEZ (2018). *Malum passionis. Mitigar el dolor del Derecho penal*, Atelier, Barcelona.

SILVA SÁNCHEZ (2013). "Teoría del delito y Derecho penal económico-empresarial". En Silva Sánchez, J.M. y Miró Llinares, F., *La teoría del delito en la práctica penal económica*. La Ley, Madrid.

SILVA SÁNCHEZ (1999). "Las inveracidades de los particulares ante el Derecho penal". En Salvador Coderch, P. y Silva Sánchez, *Simulación y deberes de veracidad. Derecho Civil y Derecho Penal: dos estudios de dogmática jurídica*. Civitas, Madrid.

SILVA SÁNCHEZ (2019). "No sólo bienes jurídicos", *InDret penal*, editorial número 3 (2019).

SOUZA DE MENEZES/AGUSTINA (2020). "Big Data, Inteligencia Artificial y policía predictiva". En D. Dupuy (dir.) M. Kiefer (coord.) *Cibercrimen III*. BdF, Buenos Aires-Montevideo, 2020, pp. 137-181.

SULER (2004). The Online Disinhibition Effect, *Cyberpsychology & Behavior*, Volume 7, Number 3, 2004. https://doi.org/10.1089/1094931041291295

TERUEL LOZANO (2019). "Derechos fundamentales en la sociedad digital: ¿Hacia una constitución para el ciberespacio?", *Revista chilena de derecho* 46.1 (2019), pp. 301-315.

VELASCO NÚÑEZ (2016). *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*. Ed. Sepin, Madrid.

VESTING (2018). *Legal theory and the media of law*. Edward Elgar Publishing.

VORMBAUM (2020). *Einführung in die moderne Strafrechtsgeschichte*, Springer-Verlag.

WALL (2001). Cybercrimes and the Internet. In D.S. Wall (ed), *Crime and the Internet*, New York: Routledge, 2001, 1-17.

WESTLAKE (2018). Delineating Victims from Perpetrators: Prosecuting Self-Produced Child Pornography in Youth Criminal Justice Systems, *International Journal of Cyber Criminology* Vol 12 Issue 1 January – June 2018, 255-268.