VI

FUNDAMENTOS DE PUNIBILIDAD E IMPUTACIÓN OBJETIVA DE LOS CIBERDELITOS: REAFIRMACIÓN DEL FUNCIONALISMO NORMATIVO

Carlos Bardavío Antón

Resumen: En una sociedad tan diferenciada, el derecho penal se dirige a responder, cada día más, a nuevas formas de criminalidad. Una de ellas está en los ciberdelitos, que se caracterizan por cometerse en un espacio muy particular: el ciberespacio. Este motivo ha dado una gran discusión doctrinal sobre la protección penal y modelos de resolución. El presente estudio aplica la teoría de sistemas y el funcionalismo normativo, para resolver los fundamentos de punibilidad e imputación objetiva de las formas criminales que se desarrollan en el ciberespacio.

Palabras clave: Ciberdelitos, cibercriminalidad, imputación objetiva, funcionalismo normativo, teoría de sistemas.

6.1 Introducción: hacia los sistemas de injusto e injustos sistémicos

Desde la mitad del siglo pasado, la cibernética[198] y la teoría de sistemas[199] han ocupado una amplia difusión en la sociología moderna y, más recientemente, en el derecho penal. El ciberespacio y su sistema, en la actualidad, suponen un nuevo ámbito de criminalidad,[200] que ha precisado de

[198] Véase, Ashby, W. R., *An introduction to cybernetics*, London, Chapman & Hall, 1956; Foerster, H., *Las semillas de la cibernética. Obras escogidas*, Barcelona, Gedisa, 1991; Wiener, N., *Cybernetics: or control and communication in the animal and the machine*, Cambridge-Massachusetts, The Massachusetts Institute of Technology, 1948.

[199] Bertalanffy, L., *Teoría general de los sistemas: Fundamentos, desarrollo, aplicaciones*. México, FCE, 1989.

[200] Sieber, U., *Computerkriminalität und Strafrecht*, Berlín, Heymann, 1977.

una respuesta penal adaptada. Ciertos delitos como el ciberterrorismo, el ciberespionaje y el acoso (*cyberstalking*, *cyberbullying*, *online harassment*) son *formas* novedosas de lo injusto.

En esta nueva modernidad, más que una sociedad globalizada, se asienta la idea de una *sociedad mundial*.[201] La interconexión de todas sus partes y de sistemas es continua y en el mismo espacio, abriendo un horizonte de posibilidades infinito, que hace que la incertidumbre del delito tienda a la posibilidad. Esta interconexión permite que, lo que antes era imposible, ahora sea posible, y esto sólo se puede entender mediante una la reinterpretación de la sociedad, de las jerarquizadas y territoriales a las que, de manera funcional, son diferenciadas. Desde esta perspectiva, la imputación de lo injusto abre nuevas posibilidades. Ahora cualquier comunicación es instantánea y se puede dar en cualquier lugar: una ventaja para la comisión de delitos. Al respecto, resulta plausible el modelo explicativo de la teoría de sistemas de Luhmann y del funcionalismo normativo.

Este tipo de criminalidad ha pasado de una primera generación de delitos informáticos, donde la protagonista era la propia herramienta informática, a un mundo cibernético, promovido por la red Internet. Lo cierto es que la diferenciación entre delitos informáticos y ciberdelitos ha sido polémica, pero, en la actualidad, parece que hay preferencia en utilizar la expresión *ciberdelitos* o *cibercrímenes*, porque incluye a los primeros.[202]

Ya sea como *delito informático* o *criminalidad mediante computadoras* (delitos con los que se ataca a un sistema informático con la repercusión material que fuere, por ejemplo, la estafa informática, y sus concursos)[203] o como *ciberdelitos* (delitos realizados a través de sistemas de comunicación virtuales, por ejemplo, internet), lo cierto es que en ambos casos se trata de *una misma comunicación delictiva*, esto es, que afectará a unos bienes u otros, dependiendo del alcance de la *interacción* del *medio* de comunicación con las personas.

En España, este auge del riesgo cibernético puede contemplarse en distintos delitos ubicados sistemáticamente en diversos ámbitos de pro-

[201] Luhmann, N., *La sociedad de la sociedad*, México, Herder, 2007, pp. 148 y ss.

[202] Romeo Casabona, C. Ma., *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006, pp. 5 y ss.

[203] Corcoy Bidasolo, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Eguzkilore*, núm. 21, 2007.

tección.[204] Estos nuevos delitos expresan, en muchos casos, la *evolución* del derecho penal, por un, lado, mediante una técnica legislativa de equivalencia a delitos tradicionales pero adaptándose a dicha fenomenología, y, por otro, mediante la anticipación de la barrera punitiva,205 lo que constata la realidad normativa del denominado *derecho penal de enemigo* como sistema punitivo diferenciado en el control de fuentes riesgosas.206 En este sentido, los denominados en la actualidad como cibercrímenes/ciberdelitos aglutinan un conjunto variado de formas de ataques207 contra distintos bienes, si bien acotados al propio campo de acción, son estrictamente comunicaciones, no lesionan en principio bienes personales tangibles —al menos, hasta la fecha—.

---

[204] Por ejemplo, los delitos de intrusión informática (CP, artículo 197 *bis*, apartado 1); interceptación de las transmisiones de datos (CP, artículo 197 bis, apartado 2); y los delitos informáticos relacionados con la propiedad intelectual e industrial (CP, artículos 197 *bis*, 197 *ter*, 197 *quater*, 197 *quinquies* y ss., y 270 y ss.); contra bienes personales como las amenazas (CP, artículos 169 y ss.); las calumnias e injurias (CP, artículo 205 y ss.); a través de cualquier medio de comunicación, producción, venta, distribución, exhibición o posesión de material pornográfico, en cuya elaboración hayan intervenido o sido utilizados menores de edad o incapaces (CP, artículo 189); la inducción a la prostitución de menores (CP, artículo 187); delitos patrimoniales como los fraudes informáticos (CP, artículo 248.2: manipulaciones del programa, introducción de datos falsos, suplantación de la identidad); el sabotaje informático (CP, artículos 263 y 264.2: tipo agravado de daños); posesión de *software* informático destinado a cometer delitos de falsedad (CP, artículos 390 y ss.); o delitos acceso ilegítimo a sistemas de comunicación y servicios (CP, artículos 255 y ss.). De manera amplia, sobre la evolución de los ciberdelitos en España, véase, Bardavío Antón, C., "Ciberdelitos: evolución hacia un derecho penal funcional incorrectamente dogmatizado", en Miguel Bustos Rubio y Alfredo Abadías Selma (dirs.), *Una década de reformas penales: análisis de diez años de cambios en el Código Penal (2010-2020)*, Barcelona, Bosch, 2020.

[205] Romeo Casabona, *op. cit.*, pp. 15 y ss.

[206] Jakobs, G., "Derecho penal del ciudadano y derecho penal del enemigo", en Günther Jakobs y Manuel Cancio Meliá, *Derecho Penal del enemigo*, Madrid, Thomson-Civitas, 2003, pp. 19-56.

[207] Por ejemplo, algunos riesgos novedosos dentro de los ciberdelitos son la *denegación de servicios* (DoS) a *servidores de sistemas* de nombres de dominio; la *desfiguración de sitios web* (*web site defacement*); la *red de ordenadores* controlados por un tercero; programas maliciosos (*ransomware*); el *phishing* como engaño al usuario para que revele una contraseña; amenazas persistentes avanzadas (*advanced persistent threat*); el *internet de las cosas* (IoT) mediante ataques a elementos domóticos o médicos; ataques a los almacenamientos de datos del *smartphone* y a los sistemas de control industrial; o casos en los que el uso de *smart contracts* sirve para producir estafas masivas.

De lo dicho, se puede ya intuir una cuestión: hay injustos que atacan sistemas y hay sistemas que acatan sistemas e injustos, esto es, *el sistema como injusto propio y como delito-medio y/o fin*, entonces, *sistemas de injusto* e *injustos sistémicos*.[208] Con esto nos referimos a dos modelos de conducta criminal. En los primeros, los sujetos utilizan la cibernética como sistema cerrado para cometer el delito contra el sistema informático, con la repercusión típica que fuere (patrimonio, propiedad intelectual, intimidad: *delitos informáticos*), y en los segundos, el sistema informático o cibernético es más abierto (sobre todo por el medio Internet) y es el propio injusto sin perjuicio de atacar a otro injusto en el medio cibernético (*ciberdelitos*).

Así pues, se trata de delimitar la *imputación objetiva*, con el objeto de precisar la responsabilidad criminal de los sujetos que intervienen en el ciberdelito. Sobre la fundamentación de esto, basta tratar la teoría de sistemas para ver dicha diferenciación.

6.2 Teoría de sistemas y el medio de comunicación del ciberespacio: protección del *ciber-espacio*

La teoría de sistemas sociales de Luhmann y su traslación al mundo jurídico, especialmente por Jakobs, sirve de modelo explicativo para la imputación de estas nuevas formas de riesgo y de criminalidad.

Para Luhmann, cada sistema (derecho, política, economía, etcétera) está *clausurado* en sus operaciones de forma *autorreferencial, autodescriptiva* y *autopoiética*[209] respecto a otros sistemas o *entornos*, pero está abierto cognitivamente (en su estructura). La diferenciación de los sistemas se realiza por la *comunicación de sentido*. Cada sistema social tiene sus propias operaciones. Estas operaciones se autorrefieren (*autorreferencia*), pero, a la vez, se autoconstruyen (*autopoiesis*), lo que causa

[208] Lampe, E. J., Injusto del sistema y sistemas de injusto, en Carlos Gómez-Jara Díez *et al.* (eds.), *La dogmática jurídico-penal entre la ontología social y el funcionalismo*, Lima, Grijley, 2003.

[209] Luhmann toma, en parte, el concepto de *autopoiesis* de Maturana, que significa *auto-creación circular* y *espontánea*. Véase, Maturana H., y Varela F., *De máquinas y seres vivos. Autopoiesis: la organización de lo vivo*, 5a. ed., Chile, Universitaria, 1988, pp. 28 y ss. Asimismo, Luhmann, de la *cibernética* de Wiener, toma el concepto de *retroalimentación* de los sistemas sociales y el concepto de *circularidad*; así como el *principio del orden a partir del ruido* de Foerster y, antes, conceptos de la *teoría general de los sistemas* de Bertalanffy. Véase, Wiener, *op. cit.*; Foerster, *op. cit.*; y Bertalanffy, *op. cit.*).

la diferenciación clausurada con otros sistemas o entornos. Además, cada sistema tiene su propio *medio de comunicación simbólicamente generalizado* para diferenciarse: el *amor* para las relaciones humanas, la *verdad* para la ciencia, el *poder* para la política, el *dinero* para la economía y lo *justo* para el derecho.[210]

Estos medios de comunicación suponen un *código positivo/negativo* que articula las operaciones en el sistema: las expectativas positivas (*fiables*) y negativas (*no fiables*). En el derecho, por ejemplo, es el *código justo/injusto*. Lo justo es lo fiable, lo injusto lo no fiable, por eso este lado negativo sirve de orientación hacia lo fiable. Sin embargo, los *sistemas psíquicos*, los pensamientos del hombre, su moral, no constituyen un elemento propio de los sistemas, sino del *entorno*.[211]

No obstante, todos debemos contar con la contingencia que suponen los otros (*alter*) en nuestras propias expectativas (*doble contingencia*), esto es, puede suceder de otra manera y lo imposible se puede hacer posible para reducir la complejidad pero, a la vez, dicha reducción *crea otra al crearse un nuevo horizonte*. Según Luhmann, esta confluencia de expectativas de unos y otros forman las *normas de deber* en la sociedad, unas veces *legales*, otras *convencionales* o *morales*. Las normas son las operaciones de las expectativas de uno (*ego*) con las del otro, *alter*,[212] son expectativas y expectativas de expectativas del otro: la fiabilidad.[213]

En este sentido, lo que nos interesa en este trabajo es un subsistema de la sociedad, el derecho y, en específico, el sistema del derecho penal, en cuyo seno se cumple su diferenciación en el código justo/injusto,

---

[210] Luhmann, Niklas, *La realidad de los medios de masas*, México, Anthropos, 2007.

[211] Por eso, la sociedad es comunicación, no consiste en individuos ni en su moral, sino en comunicaciones en una estructura (*red de expectativas*) que están en el lado objetivo de la *relación cognoscitiva*. Véase, Luhmann, Niklas, *La moral de la sociedad*, Madrid, Trotta, 2013, 91. De ahí que el sistema penal no pueda sancionar conductas reprochables moralmente, por una generalidad. En nuestro ámbito de estudio, la *pornografía simulada* o *pseudopornografía* es controvertida en nuestro ámbito de estudio.

[212] *Ibidem*, pp. 34, 96 y ss.

[213] Se pueden dar dos clases de expectativas: *cognitivas* y *normativas*. Las expectativas *cognitivas* y *normativas* se diferencian en que, con las primeras, podemos *aprender*, mientras que con las segundas *no aprendemos* o nos mostramos reacios a aprender; se da una alta fiabilidad, que, si no se cumple, es porque no era exigible tal expectativa. Véase, Luhmann, Niklas, *Sistemas sociales. Lineamientos para una teoría general*, 2a. ed., México, Anthropos, 1998, p. 104).

o más exactamente en el derecho penal, el código *punible/no punible*. De este modo, entre el sistema de injusto e injusto sistémico como delito-fin, su fundamento de conexión se halla en el *sistema de interacción* o *posibilidades de interacción*,[214] es decir, las *personas*, las cuales son las únicas capaces de producir comunicación de sentido.

Centrar así la problemática, el ciberespacio es otro *medio* de comunicación.[215] Tal y, como comenta Aguirre Romero, la "realidad es que en el ciberespacio quienes se comunican directamente son las máquinas. Son ellas las que actúan como mediadoras para posibilitar nuestras comunicaciones interpersonales".[216] Sin embargo, ellas no crean *sentido*, sólo la *interacción de las personas* puede crearlo. No podemos admitir entonces que el ciberespacio sea un sistema social[217] o *hipersistema*,[218] sino un *sistema de comunicación tecnológico* del *sentido* de los sistemas sociales, pues no tiene un medio de comunicación simbólicamente generalizado[219] como los *mass media* (informable/no informable), el derecho (justo/injusto), la política (poder/no poder), etcétera. Tal y como comenta el propio Luhmann[220] "el sistema de comunicación de la sociedad se vuelva cada vez más dependiente de los acoplamientos estructurales (tecnológicamente condicionados) con los datos de su entorno". Entonces, ahora sí, tal y como dice Aguirre Romero, las "metas del sistema tecnológico son simples: aumentar y hacer más rápido el flujo que constituye la esencia del ciberespacio: la información".[221] En nuestro ámbito de estudio, el ciberespacio se presenta como *medio de comunicación del sentido* y, entre dichos *sentidos,* caben *formas* delictivas.

Desde aquí se puede resolver que el ciberdelito es otra *forma* de lo injusto a través de su medio comunicacional: el sistema de comunicación

---

[214] Véase, Aguirre Romero, J. Ma., "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI", *Espéculo, Revista de Estudios Literarios*, Universidad Complutense de Madrid, [en línea], núm. 27, julio-octubre 2004, Formato html, Disponible en: *http://www.ucm.es/info/especulo/numero27/cibercom.html*

[215] Véase, Luhmann, La sociedad… *cit.*, pp. 234-240; Aguirre Romero, *op. cit.*

[216] Aguirre Romero, *op. cit.*

[217] *Idem*.

[218] Asencio-Guillén, A., y J. Navío-Marco, "El Ciberespacio como sistema y entorno social: una propuesta teórica a partir de Niklas Luhmann", *Communication and Society*, núm. 31, 2018, pp. 23-38.

[219] Luhmann, La sociedad… *cit.*

[220] *Ibidem*, p. 234.

[221] Aguirre Romero, *op. cit.*

tecnológico. Entonces, habrá que determinar las cualidades del sistema del derecho penal para resolver su propia diferenciación en cada acto de comunicación criminal, en nuestro caso de estudio, la comunicación en el medio de la cibernética criminal.

Al respecto, se ha dicho con gran acierto que *espacio* y *tiempo* alcanzan otra dimensión en el ciberespacio y afectan de forma decisiva a la *oportunidad delictiva* (tipología de autores, motivación, eficacia, bienes jurídicos, tipología y pluralidad de víctimas), la *deslocalización*, *transnacionalidad*, *neutralidad* y la *descentralización* del delito, pero también, la *popularización* y *anonimización* a un *ciberespacio abierto* sujeto a *revolución permanente*,[222] esto es, el medio cibernético está expuesto a constante *innovación*.

Sin embargo, esto sólo supone otra nueva constatación de la propia funcionalidad de los sistemas, es decir, los sistemas operan con un tiempo y espacio ajeno al del mundo natural.[223] Entonces, lo que demuestra el ciberespacio es que la comunicación siempre está en estado *atemporal y aterritorial,* con los problemas de inicio, imputación delictiva y de competencia que acarrea esto en determinados delitos (acción, resultado, oportunidad o ubicuidad),[224] pero que ahora se puede resolver mediante el siguiente *axioma*: hay sistema de comunicación.

La comunicación siempre es posible porque está en todo momento disponible en una *sociedad mundial*,[225] en un mismo espacio, con tiempos modificables, lo que lleva a considerar la comunicación como un derecho fundamental (*institución protectora de la diferenciación*) y, el delito, su *contrafactum*. La comunicación siempre está ahí en la sociedad, es por

---

[222] Miró Llinares comenta que "lo que esto quiere decir es que cualquier agente en el ciberespacio, salvo el impedimento del contacto físico directo, tiene menos restricciones espaciales y temporales para sus actos que en el espacio físico. También, que los efectos de las conductas, las consecuencias plasmadas en unas coordenadas espacio/temporales determinadas, *ofrecen menor información en el ciberespacio* de las coordenadas espacio/temporales del acto al que se deben atribuir las mismas y, por ello, del agente causante, que en el espacio físico" (la cursiva es nuestra). Véase, Miró Llinares, F., *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, p. 10.

[223] Luhmann, Niklas, *Organización y decisión*. México, Herder, 2010, p. 206.

[224] Romeo Casabona, *op. cit.*, pp. 31-37.

[225] De aquí la importancia de la *constitucionalización sin Estado* (Teubner, 2005, pp. 92-95), de la *constitución digital* (Teubner, 2005, pp. 105-118) y del *derecho penal internacional*, por ejemplo, el *Convenio sobre la ciberdelincuencia*.

eso que, en la actualidad, es muy probable ser víctima de ciertos delitos en los que antes era casi imposible caer.

El ciberespacio demuestra que el espacio de la comunicación (del delito) *tiende a 0* como un factor de la posibilidad del todo y, concretamente, de la comunicación criminal. Las *instalaciones de registro* "permiten diferentes disposiciones de tiempo en ambos lados y con ello (…) más fácil la realización de las comunicaciones".[226] Por eso, en un espacio 0, el *tiempo* también puede entenderse como una *reducción de la complejidad*,[227] en nuestro ámbito de estudio, reducir la complejidad para cometer el delito. Por eso no debe sorprender que las nuevas constataciones de la autonomía del tiempo y del espacio en los cibercrímenes sea incluso redundante, porque tales medidas son siempre diferentes de la realidad física. Pero, hay más, dicho tiempo/espacio propicia en el ciberespacio que se cree un ámbito en donde los sistemas sociales producen más acusadamente la *inclusión* y la *exclusión*[228] —de las personas— en ese lugar de comunicación.

En este sentido, el ciberespacio ha servido de *reductor de la complejidad cotidiana* de la comunicación que, a su vez, ha creado un *nuevo horizonte de expectativas* para el criminal, dicho de otra manera, esta reducción de complejidad ha creado otras: los ciberdelitos, los cuales pueden dar resultados más intensos, nuevos objetos materiales y formas comisivas,[229] que precisan de unas fórmulas preventivas (tipos) pero también nuevas fórmulas de valoración; la imputación objetiva, mediante *reglas flexibles* que respondan a los cambios de dichos entornos (comportamientos/operaciones/comunicaciones) capaces de ser recogidas por el código punible/no punible.

Se suele decir que los ciberdelitos no tienen un bien jurídico protegido común, sino que tratan de un modo de riesgo por la utilización de In-

[226] Luhmann, La sociedad… *cit.*, p. 234.

[227] *Ibidem*, p. 25.

[228] Teubner, *op. cit.*, pp. 115-116. Añade, en coherencia, que las "expectativas normativas relativas a modalidades de conducta, que siempre pudieron ser interpretadas, adaptadas, manipuladas, desviadas, se convierten en rígidas expectativas cognitivas de situaciones fácticas (inclusión/exclusión) […] No es extraño que en tal situación […] la figura del *hacker* […] se convierta prácticamente en un mito de Robin Hood".

[229] González Rus, J. J., "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", *Delito e informática: algunos aspectos*, Bilbao, Publicaciones de la Universidad de Deusto, 2007, pp. 33 y ss.

ternet.[230] Por ejemplo, Romeo Casabona[231] explica que este tipo de delitos protegen de manera intensa la *comunicación*. Rovira del Canto,[232] por su parte, centra la protección en la *información*. En nuestra opinión, lo que se trata de proteger con estos delitos es al propio ciberespacio, pues tanto comunicación como información se dan siempre como objeto de protección, el sentido, pero diferencialmente en este caso se protege su concreto *espacio* en el que se desarrollan. De aquí que un concepto unívoco de *delito informático* o de *ciberdelito*, siguiendo la teoría tradicional, sea imposible y, por lo tanto, tampoco puede tratarse de un bien jurídico específico,[233] sino, en nuestra opinión, de su medio de comunicación: el *espacio(-ciber)*.

No se puede reducir el ciberdelito a un ataque a la *seguridad* o *confianza* como bien jurídico colectivo. Cualquier delito ataca siempre algo mayor que la estricta materialidad del daño que fuere: la *vigencia de la norma*.[234] Pero este resultado no es incompatible con que la vigencia de la norma, medial y secundariamente, protege bienes jurídicos. En los ciberdelitos esto se refieren a un conjunto *heterogéneo* de bienes mediante la utilización de la cibernética y/o atacando a ésta, por lo que en verdad el elemento común es la cibernética. Dicha *heterogeneidad* deviene precisamente del *mundo de posibilidades* criminales que ofrece el ciberespacio y de los nuevos postulados actualizados a dicho medio que se refieren a *formas* normativas (violencia, intimidación, patrimonio, etcétera).

Así pues, el derecho penal lo que trata de proteger es el ámbito funcional y estructural del ciberespacio, la vigencia de la norma que confluye en el medio comunicacional del espacio (*-ciber*), es decir, a esta *máquina invisible* y, de tal modo, al ámbito de comportamientos libres de las personas en ese espacio: se protege un *espacio virtual de comunicación* y *medialmente a bienes jurídicos* de índole heterogéneo. Al igual que se protege el sistema socioeconómico en diversidad de delitos sin perjuicio de bienes más concreto o personales, el sistema del ciberespacio es protegido en su ámbito de actuación sin renunciar a esferas concretas, por

---

[230] Barrio Andrés, *op. cit.*, pp. 26-27

[231] Romero Casabona, *op. cit.*, pp. 187-190.

[232] Rovira del Canto, E., *Delincuencia informática y fraudes informáticos*, Granada, Comares, 2002, pp. 70 y ss.

[233] González Rus, *op. cit.*, pp. 14 y ss.

[234] Véase, Jakobs, G., *Derecho penal. Parte general. Fundamentos y teoría de la imputación*, Madrid, Marcial Pons, 1997.

ejemplo, la intimidad, pero con importantes repercusiones en la *epistemología* normativa, en la autonomía individual e institucional.[235]

Desde esta perspectiva está claro que el derecho penal trata de proteger ese *espacio (-ciber)*. Lo problemático hasta ahora era resolver cómo lo protege. En nuestra opinión sólo es posible aceptando los postulados sistémicos explicados y mediante su *autodescripción*, esto es, mediante la *imputación objetiva*. Entonces, se precisa analizar la teoría de la imputación objetiva desde las fórmulas del funcionalismo normativo, al objeto de comprobar su aplicabilidad a la cibercriminalidad, sin incurrir en un derecho penal funcional incorrectamente dogmatizado, como parece que está sucediendo con los diversos tipos en cuestión (Bardavío Antón 2020a).

6.3 Imputación objetiva: aplicabilidad del funcionalismo normativo

6.3.1 Introducción

El sistema del derecho penal es un acontecimiento social que interpreta el significado de un comportamiento, su sentido y, por lo tanto, trata de la operación autodescriptiva de la imputación del *significado del comportamiento*.[236] Entonces, la imputación objetiva reúne la imputación del *lado subjetivo* como *símbolos* de acontecimientos y sólo "en tanto que relación con el significado de comportamiento (…) en cuanto portador de una expresión de sentido de la persona, es que los hechos psíquicos (…) pertenecen al hecho punible",[237] pues sólo de esta manera cumple con su operatividad (imputación) en la forma del código justo/injusto o más precisamente punible/no punible.

---

[235] Teubner, *op. cit.*, p. 115, comenta que la "digitalización […] produce una especie de fusión nuclear de creación, aplicación y ejecución del derecho […] desaparece una división de poderes constitucional dentro del proceso jurídico y una importante garantía para los espacios de autonomía individual e institucional".

[236] Jakobs insiste en que el "significado de un comportamiento sólo puede determinarse a la vista de su posición en el contexto social […] Esta interpretación en un contexto social del comportamiento unido a sus consecuencias causales o incluso a sus consecuencias causales anticipadas, se lleva a efecto en la dogmática moderna bajo el nombre de "imputación objetiva", que aquí se denominará la teoría del significado del comportamiento". Véase, Jakobs, G., "La imputación jurídico-penal y las condiciones de vigencia de la norma", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Granada, Comares, 2005, pp. 186-187.

[237] *Ibidem*, p. 191.

Si hablamos de imputación objetiva, es al objeto de precisar la operación de entrada de la comunicación criminal en el ámbito del sistema social del derecho penal. Luego entonces, la imputación objetiva es la operación por la cual el sistema *reconoce* a dicha comunicación que produce el *sistema de interacción* —del autor, víctima y terceros— como propia, en sí, es una *forma* de *autodescripción* de la *estructura normativa* del sistema penal[238] que además se *heterorrefiere* a toda la sociedad (confianza, riesgos tolerables, tiempo, etcétera), pero de un modo particular, transformando también dicha heterorreferencia en autorreferencia, por ejemplo: riesgos permitidos y no permitidos en el derecho penal.

En este sentido, no sólo la norma es una autodescripción del sistema penal de su vigencia (*seguridad de la orientación de la conducta)*,[239] sino también la pena.[240] De este modo la conducta criminal supone una *comunicación de sentido contrafáctica* de la autodescripción del sistema penal, de la vigencia de la norma, que se solventa por el sistema mediante la vigencia de la pena. Por eso es de especial trascendencia la imputación objetiva como *forma estructural* y *contextual* (autorreferencia y heterorreferencia respectivamente) de reconocimiento de dicho tipo comunicación (autodescripción) y, de ahí, las formas de aseguramiento contrafáctico mediante la pena (otra autodescripción).

Trascendencia de lo anterior es que la imputación objetiva de cualquier delito se basa en la diferenciación del código punible/no punible, y no en el causalismo analítico del sistema psíquico (personas) basado en la progresividad de la teoría del delito (tipicidad, antijuricidad, culpabilidad, exigibilidad, punibilidad).[241] Es decir, dicho código manifiesta si se

---

[238] Müssig, B., "Aspectos teórico-jurídicos y teórico-sociales de la imputación objetiva en derecho penal. Puntos de partida para una sistematización", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Granada, Comares, 2005, pp. 197-198.

Véase, Luhmann, N., *El derecho de la sociedad*, 2a. ed., México, Universidad Iberoamericana/Biblioteca Francisco Xavier Clavigero/Herder, 2005.

[240] Jakobs, G., "Sobre la teoría de la pena", *Bases para una teoría funcional del derecho penal*, Lima, Palestra Editores, 2000, pp. 59-108; y Müssig, *op. cit.*, pp. 197-198.

[241] En este sentido, Luhmann ya apuntaba alto: "por eso se propone concebir la causalidad como esquema de un observador, es decir, como un médium, sobre el cual un observador delinea formas. El médium se construye mediante los posibles factores causales (siempre, y al mismo tiempo: causas y efectos; las formas surgen al distinguir el observador causas y efectos, seleccionar las causas o efectos que le son interesantes y acoplarlos concretamente". Véase, Luhmann, Organización… *cit.*, p. 215.

ha producido una comunicación en el ámbito concreto del sistema o no, sin perjuicio de que la comunicación pueda también resultar en otros sistemas (otro sentido). También la *imputación ordinaria* y *extraordinaria* desarrollada por Hruschka[242] sigue siendo imputación.

Amén de ello, la *forma* es aquí la *operación sobre cada elemento de la imputación objetiva*, que se reconozca o no como *diferencia* sin necesidad de entrar en el causalismo de la teoría tradicional del delito. Así, dichas categorías del delito, por ejemplo, el hecho criminal (modos, motivos, fin, *quantum*, etcétera): distinciones en la *capacidad de imponerse y fugacidad temporal de la forma*[243] se reconocen como *formas del medio de comunicación penal*, esto es, no sólo el tipo objetivo (controlabilidad/evitabilidad), sino también el tipo subjetivo. La antijuricidad y la culpabilidad son, entonces, *autodescripciones* del sistema penal,[244] y sus formas se acoplan a éste con mayor o menor rigidez. No se ve la luz sino las cosas,[245] entonces no se ve la tipicidad sino su forma, por ejemplo, que un sujeto mate a otro *con relevancia penal*, y así en cada autodescripción condensada en el código punible/no punible.

Al respecto, Posada Maya[246] comenta acertadamente que el ciberespacio ha cambiado la valoración de la acción típica física a la *ciberacción* (dificulta la determinación del tiempo y lugar de los delitos), crea problemas sobre el conocimiento del dolo en acciones programables y automatizadas o de inteligencia artificial, también en el tradicional concepto de dominio objetivo y positivo del hecho, en la tipicidad con una perspectiva digital y en las organizaciones virtuales transnacionales (OVT).[247]

---

[242] Hruschka, J., *Strafrecht nach logisch-analytischer methode*, 2a. ed., Berlín-Boston, De Gruyter, 1988.

[243] Luhmann, La realidad de… *cit.*, p. 153.

[244] Bleckmann, *op. cit.*, pp. 361-376; Jakobs, La imputación… *cit.*

[245] Luhmann, La sociedad… *cit.*, p. 154

[246] Posada Maya, R., "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", *Revista Nuevo Foro Penal*, núm. 13, 88, enero-junio, 2017, pp. 106-107.

[247] En este sentido, Maya Posada subraya que las OVT están "constituidos por un número indeterminado y concatenado de procesos informáticos ilícitos (medio-intermedios o preparatorios)". Véase, "¿Puede ser el cibercrimen un delito organizado y transnacional?", en Juan Carlos Rodas Montoya (ed.), *Temas de derecho penal económico y patrimonial*, Medellín, Universidad Pontificia Bolivariana, 2018, p. 246

Y es que con el ciberespacio (*médium*) se puede realizar cualquier delito si se transforma el tradicional concepto de materialidad del espacio al de *virtualidad* en sí: *comunicación*.[248] Entonces, el delito se produce en un mismo espacio o, dicho de otra forma, *en todo ese espacio*, pues el concreto espacio físico donde se refleja lo injusto (por ejemplo, en la acción o en el resultado) *contiene todos los demás espacios*.

En concreto, las categorías señaladas en la teoría moderna de la imputación objetiva —que luego analizaremos—, responden a cualidades *formales* de dicha operación de *reconocimiento del médium de comunicación delictiva*. La cuestión a resolver es cómo este nuevo medio de comunicación criminal se resuelve por el código punible/no punible mediante las *formas* de la *imputación objetiva.*

Pues bien, este tipo de delitos producen cierta *simultaneidad* pero también produce la probabilidad de la *continuidad*.[249] Sin embargo, estas comunicaciones delictivas pueden ser divididas temporalmente mediante *formas* (actos preparatorios, tentativa, consumación). Cada forma en la progresividad delictiva se refiere también a su continuidad hasta alcanzar la nueva fase, y esto se debe a que la comunicación formal puede ser dividida en *fases*,[250] lo cual puede trasladarse también al sistema penal: información/diferencia (preparación), envío (tentativa inacabada/ *dar-a-conocer*), aceptación de la comunicación (tentativa acabada) y entendimiento del sentido (consumación), entonces, estas fases se refieren al tipo penal.[251] Así pues, cada *forma* temporal de la imputación objetiva

[248] También lo dicho lleva a preguntarnos sobre otra posibilidad: la adaptación de conceptos normativos a la nueva realidad comunicativa, por ejemplo, el concepto de *violencia*, ¿Se puede agredir sexualmente por internet? Desde una concepción tradicionalista del derecho penal, basada en bienes jurídicos diferenciados en su materialidad, desde luego que no, pero, con los nuevos planteamientos que estamos esgrimiendo, podemos aceptar dicha posibilidad. Falta poco para apreciar que quien, a través de internet, mediante *violencia coactiva* o doblegando la voluntad del consentimiento de un sujeto, lo obliga a introducirse un objeto por vía vaginal o anal, para que pueda considerarse un delito de violación en *autoría mediata dual*. O, respecto a la superioridad numérica, como forma de *intimidación* (también en casos especiales como violencia, mediante la presencia de gran número de internautas en una retransmisión *online* cerrada), en estos casos pueda aparecer el fundamento de la violación.

[249] Tiedemann, K., "Criminalidad mediante computadoras", *Nuevo foro penal*, Bogotá, núm. 30, octubre-diciembre, 1985, p. 126.

[250] Luhmann, La sociedad… *cit.*, pp. 145-155.

[251] Bleckmann, *op. cit.*, p. 361.

alcanza mayor o menor aplicación según el *medio* (en nuestro caso muy intenso: ciberespacio) y el entorno (contexto).[252]

Así las cosas, nos vamos a centrar en analizar operaciones de *autodescripción* del sistema penal como elementos de la imputación objetiva del mismo: tipología de riesgos y roles, autopuesta y heteropuesta en peligro, confianza, prohibición de regreso, competencia en la organización e infracción de deber, el tiempo (tentativa, consumación y resultados tardíos) y el sistema de injusto y los injustos sistémicos (en la autoría, participación, organización criminal y en la persona jurídica).

6.3.2 Riesgo no permitido y neutro: quebrantamiento del rol común y especial

La sociedad para poder funcionar necesita de contacto e, incluso, que ciertos contactos riesgosos sean permitidos. Hay cierta permisividad social en riesgos, se toleran y socialmente son adecuados. Los *riesgos permitidos* son aquéllos que son imprescindibles para el funcionamiento de la sociedad.253 De ahí que se deban asumir las consecuencias de la *autopuesta en peligro*, salvo que un tercero quebrante un riesgo no permitido.

En este sentido, la creación de un riesgo no permitido o la *no neutralización de un riesgo*254 supone el quebrantamiento del rol común (rol básico de persona: no dañar) o especial (rol según un contexto especial:

---

[252] Al respecto, Luhmann señala que "se abandona la unidad de dar-a-conocer y entender. Quien ingresa algún dato no sabe (y si lo supiera no tendría necesidad de la computadora) lo que será extraído por el otro lado […] En nuestra conceptuación esto significa […] un nuevo médium cuyas formas ahora dependen de programas de computadoras". Véase, Luhmann, La sociedad… *cit*., pp. 239-240. De aquí que "dada la diferente naturaleza de los dos mundos, *todo* usuario asume una nueva identidad para su participación en el ciberespacio". Véase, Aguirre Romeo, *op. cit*.

[253] Véase, Jakobs, G., *La imputación objetiva en derecho penal*, Madrid, Civitas, 1996, pp. 118 y ss; Jakobs, G., *Estudios de derecho penal*, Madrid, Civitas, 1997, p. 212; Luhmann, El derecho de la… *cit*., pp. 181 y ss; Maraver Gómez, M., *El principio de confianza en derecho penal. Un estudio sobre la aplicación del principio de autorresponsabilidad en la teoría de la imputación objetiva*, Madrid, Civitas, 2009, pp. 360 y ss; Piña Rochefort, J. I., *Rol social y sistema de imputación. Una aproximación sociológica a la función del derecho penal*, Barcelona, Bosch, 2005, p. 394; Polaino Navarrete, M., *Lecciones de derecho penal. Parte general*, 2a. ed., Madrid, Tecnos, 2016, t. II, p. 105; y Polaino-Orts, M., "Imputación objetiva: esencia y significado", *Imputación objetiva e imputación subjetiva en derecho penal*, Perú, Grijley, 2009, pp. 43 y ss.

[254] Polaino Navarrete, *op. cit.*, p. 106

juez, padre), el sustrato de la imputación objetiva en los delitos dolosos e imprudentes,[255] es decir, no puede *instrumentalizarse el rol* cuando las circunstancias han variado, porque las *circunstancias* (espacio, tiempo, etcétera) operan como *entorno* del sistema (el rol) y producen entradas que varían las funciones de éste: *variación del rol*.[256] Sin embargo, de este quebrantamiento no se responderá de cuantas consecuencias lesivas se produzcan, sólo de las que competen al rol (común o especial), y no en todas las circunstancias. Sólo es imputable a los sujetos el quebrantamiento de la expectativa que forme parte de su *forma rol común* o *especial*: ámbito de competencia.[257]

De lo dicho se extrae que el ciberespacio es un ámbito jurídicamente *neutro* pero, a la vez, de constante *interacción*, lo cual significa un *mundo* lleno de horizontes y de alternativas en el comportamiento.

Así pues, en los delitos de ciberterrorismo, por ejemplo, los ataques a los sistemas de seguridad informáticos de un Estado, la preparación del delito es permanente en tanto a *ciberpreparación* se refiere —ahí queda constante el peligro—, pues la construcción del ordenador o su compra para luego atacar, si bien no rebasa la *neutralidad* de dicha conducta (*cotidianidad*), sí es superada cuando se prepara un programa informático con potencialidad para destruir sistemas, por ejemplo, violar el nivel de seguridad de un Estado o las estafas informáticas (críticamente respecto a la equiparación punitiva de actos preparatorios con consumativos de la estafa informática).[258] Esto se debe a que dicho acto ya ha producido comunicación relevante, aunque se entienda que dicho programa no está aún en el ciberespacio (nube, etcétera), pues su propia configuración como sistema de ataque supone un *sistema de injusto virtual,* con tanta peligrosidad, en ciertos casos, como una organización criminal formada por personas.

En este sentido, el tipo de ataque señalado lo puede realizar tanto una persona ejerciendo su rol común de persona e incumpliendo el axioma *no dañar* (el ciberterrorista), así como un rol especial, el que tiene

---

[255] Véase, Jakobs, Estudios de… *cit.*, 7/39; y Piña Rochefort, *op. cit.*, p. 398.

[256] Piña Rochefort, *op. cit.*, pp. 402 y ss.

[257] Polaino Navarrete, *op. cit.*, p. 90; Polaino-Orts, *op. cit.*, pp. 35 y ss; Requena Juliani, J., *Intercambiabilidad de acción y omisión en los delitos de dominio: posición de garante e imputación objetiva*, Madrid, Dykinson, 2010, pp. 147 y ss.

[258] Corcoy Bidasolo, *Delitos de peligro y protección de bienes jurídico-penales supraindividuales: nuevas formas de delincuencia y reinterpretación de tipos penales clásicos*, Valencia, Tirant lo Blanch, 1999, p. 16.

deber específico de asegurar y lo incumple (el policía). En ambos casos, el riesgo permitido y no permitido se concreta en cada competencia, lo cual, a la vez, delimitará también la inclusión o exclusión de la imputación objetiva de ciertos delitos y, por ende, la autoría y participación.

6.3.3 Autopuesta y heteropuesta en peligro en el ciberespacio: imputación a la víctima

En la *sociedad del riesgo* la libertad tiene consecuencias: la responsabilidad de cada uno por sus actos (gestión del riesgo). El consentimiento de la víctima a la acción peligrosa o en las consecuencias del riesgo que puede dar a la *autorresponsabilidad de la víctima*,[259] salvo que se limite o se anule la capacidad de libertad de voluntad o de decisión de la víctima, en cuyo caso estaremos en una *heteropuesta* en peligro: heterolesión,[260] esto significa que la resolución del problema entre una autopuesta en peligro y su participación, y una heteropuesta y su participación, pasa por la *validez del libre comportamiento/consentimiento*.

Por ejemplo, la exposición de la víctima en el ciberespacio sin medidas de seguridad (aleatoriamente la víctima presta sus datos sin leer el contrato y sus consecuencias) se asemeja a los efectos de cuando un ciudadano deja la puerta de su vivienda abierta (*plus de seguridad*),[261] es decir, ciertas imputaciones no serán posibles por el propio comportamiento libre de la víctima; o en casos de páginas web o correos electrónicos destinados a engañar para que se realice una disposición patrimonial, concluye Corcoy Bidasolo, "no puede afirmarse que el engaño sea idóneo *ex ante* para provocar el error, por consiguiente, no puede calificarse como tentativa de estafa múltiple".[262]

---

[259] Véase, Cancio Meliá, M., *Conducta de la víctima e imputación objetiva en derecho penal. Estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas*, 2a. ed., Barcelona, Bosch, 2001, p. 174; y Jakobs, Estudios de derecho... *cit.*, pp. 7, 126 y ss.

[260] Véase, Cancio Meliá, *op. cit.*, pp. 284 y ss; Caro John, J. A., *La imputación objetiva en la participación delictiva*, Lima, Grijley, 2009; Polaino Navarrete, *op. cit.*, pp. 106-108; Polaino-Orts, *op. cit.*, pp. 50 y ss; Roxin, Claus, *Problemas básicos de derecho penal*, Madrid, Reus, 1976, pp. 181-199.

[261] Caro John, J. A., "Derecho penal del enemigo: garantía estatal de una 'libertad real' del ciudadano. Una glosa a Miguel Polaino-Orts", *Cuadernos de Derecho Judicial*, núm. 91, 2007, p. 264.

[262] Corcoy Bidasolo, *op. cit.*, p. 29

6.3.4 Confianza

El fundamento sobre el que gira el contacto social es la confianza, la cual, es una expectativa social generalizada de que los demás manejan su libertad de manera previsiva, lo que hace que se reduzca la complejidad social, anticipa el futuro o lo condiciona para ser utilizado en el presente con seguridad.[263] Las personas depositan confianza en los comportamientos futuros de los demás (*confianza intersubjetiva/personal*), también en cómo se aplicará una norma (confianza en el sistema normativo). A la postre, la confianza produce reglas normativas y, a la inversa, las normas posibilitan la confianza de las personas en que su comportamiento es *seguro* (o un riesgo permitido). Entonces, la confianza configura ámbitos de responsabilidad,[264] especialmente en el deber de cuidado/protección y sirve, entonces, de heterorreferencia en la autodescripción de la imputación objetiva.

Amén de esto, no puede concluirse que los ciberdelitos protegen un bien jurídico determinado en la confianza, pues ésta se *autorrefiere* —y se da— en todo el sistema social, así como en el derecho penal. Es una autodescripción inherente a la pertenencia a un sistema social mayor al que se heterorrefiere constantemente: la sociedad.

Lo problemático del principio de confianza estriba en las *relaciones especiales*. Por ejemplo, en el cuidado de los niños la confianza social es menor, por eso la expectativa normativa exige un mayor cuidado, sin embargo, también existe confianza en *relaciones normales*.

También existe diferencia entre la confianza especial que se deriva del deber de garante en la *asunción de la responsabilidad por organización* y la *confianza especial en la responsabilidad institucional*. En nuestra opinión, en las *relaciones cibernéticas*[265] no sólo puede haber responsabilidad por incumplimiento del mandato *no dañar* (*neminem laedere*)

---

[263] Luhmann, El derecho de… *cit*., pp. 39 y ss.

[264] Véase, Jakobs, Estudios de… *cit*., pp. 209 y ss; Piña Rochefort, *op. cit*., pp. 376-393; Polaino-Orts, *op. cit*., pp. 56 y ss.

[265] En este sentido, como bien razona Luhmann, la confianza se relaciona como posibilidad de adoptar una decisión, de otro modo, se habla de *esperanza*. La confianza refleja la posibilidad de que las cosas pueden suceder de otra manera, pero se adopta una decisión tomando en cuenta esas otras posibilidades (contingencia), mientras que la esperanza las elimina, por eso *la confianza también puede ser imprudente*. En estos términos, es verdad lo que dice Luhmann, el problema no es quién gana la confianza, sino cómo se gana. Entonces ese *cómo* es el fundamento del injusto. Véase, Luhmann, N., *La confianza*, México, Anthropos, 2005, pp. 40-41, 105.

referido a cualquier rol común o por organización (deberes de relación o injerencia), sino también la creación de una *confianza especial* por *asunción de un deber* puede generar una responsabilidad institucional.[266]

En nuestro ámbito de estudio, la confianza cobra relevancia, por ejemplo, respecto a la depositada en los *guardianes del ciberespacio*, aquellos encargados de proteger a la víctima.[267] Sobre esto volveremos *infra,* al tratar la autoría y participación.

6.3.5 Prohibición de regreso

La prohibición de regreso elimina la imputación objetiva de aquellos comportamientos del rol aparentemente delictivos en los que previamente el sujeto realiza una conducta neutral, exigida o normativa dentro de las competencias de su rol, aun cuando el sujeto tuviera el conocimiento (especial) de que su aportación al hecho fuese a ser empleada por un tercero para la comisión delictiva. Sin embargo, excedería del riesgo permitido, o no supondría una conducta neutral, si previamente el sujeto *modifica* el *destino* buscando no sólo la participación con el tercero, sino también la exención de responsabilidad, alegando dicha prohibición de regreso.[268]

En nuestro caso, a quien paga un servicio de pornografía online adulta no se le podrá reprochar que luego esa cantidad se destine por el servidor a pornografía infantil, a pesar de que conozca dicho destino (conocimiento especial, extra-rol). Al ciudadano no se le puede exigir que sea garante de toda consecuencia de su obrar, sólo de las que formen parte de su rol, no en todos los casos. De aquí se precisa que lo normativo es una *autodescripción* de la imputación objetiva, de manera que excluye operaciones basadas en las suspicacias de la moral del observador.

6.3.6 Delitos de organización y de infracción de deber en los ciberdelitos

La operación de la autodescripción de la imputación objetiva del sistema penal también se refiere, como decíamos *supra*, a la *competencia por organización* o *institucional*, en este último caso, por *configuración jurí-*

[266] Véase, Sánchez-Vera, J., *Delito de infracción de deber y participación delictiva*, Barcelona, Marcial Pons, 2002, pp. 183 y ss; y Jakobs, Derecho penal… *cit.*, pp. 28, 13 y ss.

[267] Miró Llinares, *op. cit.*, pp. 34 y ss.

[268] Jakobs, Estudios de derecho… *cit.*, p. 236.

dicamente garantizada u *horizontes normativos especiales*.[269] En ambos casos nos remiten al fundamento de los deberes de la *persona* en cuanto rol común o especial.

Tal y como hemos anticipado, la cuestión fundamental que nos atañe es que la *convivencia/relación* genera *deberes por asunción*, pero sólo surgiría la confianza especial cuando se promete el auxilio y se llevan a cabo actos claros de preparación para, en su caso, cumplir el deber. También en la unión de ámbitos de organización como en la *comunidad del riesgo* en la que se acuerda el auxilio mutuo, en la *estrecha comunidad de vida* (por estrecha relación familiar, amistosa o sentimental) o en la denominada *comunidad de intereses* (en la relaciones de novios, parejas de hecho), se está obligado a la evitación de riesgos vitales en la que existen riesgos mayores a los normales, cuya obligación surge de la superación común: sustitución de la confianza especial de la protección estatal.[270] En estos casos nace una expectativa social como *fuente de deber*, donde el acuerdo puede ser incluso *tácito* (la *especial relación de lealtad* entre comerciantes)[271] y su infracción representa el quebrantamiento de una *garantía*.

La *asunción de un deber* supone el inicio de una competencia del rol denominada *responsabilidad por asunción*, que además puede liberar a quien previamente ha tenido dicha competencia al tratarse de una confianza *cualificada* o *especial*, lo cual crea una *incumbencia institucional* con el mismo fundamento que la injerencia,[272] pero en este caso por una *expectativa cognitiva*, no normativa, pues esta última se garantiza de manera jurídica. En la cognitiva existe una *conexión fáctica*, una promesa de una prestación *expresa* o *concluyente*, donde el tercero deja de asumir la protección, todo ello salvo que esté viciada dicha asunción.[273] Sin embargo, los deberes por responsabilidad institucional, en sentido estricto, se equiparan a deberes de comisión por la importancia básica

[269] Müssig, *op. cit.*, pp. 208-221.

[270] Jakobs, Derecho penal… *cit.*, pp. 29, 70 y 106; Piña Rochefort, *op. cit.*, p. 405.

[271] Welzel, H., *Derecho penal alemán. Parte general*, 2a. ed., Santiago de Chile, Jurídica de Chile, 1976, pp. 300-301

[272] Jakobs, Derecho penal… *cit.*, pp. 29-52; Polaino Navarrete, M., *Acción, omisión y sujetos en la teoría del delito. De la posición de garante a la responsabilidad penal de las personas jurídicas*. Perú, Grijley, 2009, p. 91

[273] Jakobs, Derecho penal… *cit.*, pp. 29-47; Maraver Gómez, *op. cit.*, pp. 126 y ss; Piña Rochefort, *op. cit.*, pp. 418-419

de la existencia de la sociedad, como las relaciones paterno-filiales, la confianza especial y los deberes estatales.[274]

Así las cosas, en las relaciones cibernéticas se pueden quebrantar como un deber básico de no dañar o como una confianza especial, esto dependerá de cada relación, siendo problemática —como veremos— en la relación usuario/*prestador de servicios* en el ciberespacio.

6.3.7 Tentativa, consumación e imputación de los resultados tardíos

El tiempo, como decíamos, sirve de heterorreferencia en la autodescripción de la imputación del delito. En este sentido, el tiempo marca de forma decisiva ámbitos de imputación (preparación, tentativa, consumación y resultados posteriores), cuestión que es precisa analizar en los ciberdelitos.

Partimos de la base funcionalista de que la tentativa es un injusto cualitativamente de igual calado que la consumación porque aquélla también quebranta la vigencia de la norma.[275] Sin embargo, comenta Corcoy Bidasolo que, "surge una política criminal extensiva en la que se castigan actos preparatorios, en unos casos, y de cooperación, posteriores al inicio de la ejecución, en otros, que dificultan la aplicación de los esquemas clásicos".[276] Por ejemplo, en relación con delitos de *peligro abstracto* del artículo 270.3[277] considera que "1o. No necesariamente se dará la inmediatez temporal que requiere la tentativa; 2a. Será regla, casi general, que los autores de estos actos preparatorios sean diferentes de aquellos que copien o plagien el programa".

---

[274] Jakobs, Derecho penal… *cit.*, 29/58; Lesch, H. H., *Das problem der sukzessiven beihilfe*, Frankfurt-New York, P. Lang, 1992, pp. 298 y ss; Piña Rochefort, *op. cit.*, pp. 419-421; Sánchez-Vera, *op. cit.*, pp. 65 y ss.

[275] Jakobs, Derecho penal… *cit.*, pp. 25-15.

[276] Corcoy Bidasolo añade que "así, por ejemplo, la conducta de prestadores de servicios que transmiten datos o definen destinatarios se trata de un supuesto de participación posterior a la creación de los datos pero que se produce con anterioridad a la consumación y, en muchos casos, sin connivencia con el autor. Ello es así porque la consumación requerirá, en unos casos, el acceso a los datos –datos personales o pornografía– y, en otros, que el engaño produzca un error en el destinatario y éste realice la disposición patrimonial, y el envío a los destinatarios, e incluso la selección de éstos, depende de los prestadores de servicios". Véase, Corcoy Bidasolo, Problemática… *cit.*, p. 28.

[277] *Ibidem*, p. 29.

Por otro lado, Jakobs[278] considera que no pueden formularse reglas fijas para apreciar el inicio de la tentativa sino, únicamente, *directrices generales*, las cuales nos sirven para aplicarlas a los ciberdelitos y fundamentan la autodescripción de la imputación basada en heterorreferencias temporales:

a) Que *la acción se aproxime a la consumación según la representación/descuido del autor*. De este modo, el concepto de *inmediatez* ha de ser entendido mediante la objetivación del criterio subjetivo del plan/representación/descuido del autor en el ciberespacio, y esto sólo puede efectuarse analizando el ámbito de organización concreto, el rol y su competencia en dicho espacio.

b) Que *la acción sea ya la propia acción de ejecución*. Jakobs afirma que no es tentativa —generalmente— dirigirse al lugar del delito. Habrá que analizar la configuración social de dicha acción para discernir entre un acto preparatorio o una tentativa (caso *bolas de pimienta*),[279] en nuestro caso, por ejemplo, entrar en el ciberespacio con conocimientos para infectar una red es neutro, se tendrá que insertar un dato desconocido por la víctima para alcanzar alguna relevancia.

c) Una *proximidad temporal sin interrupción*. Una alta diferencia temporal entre acción y resultado no impide el inicio de tentativa, pues quien intenta puede haber planeado —también imprudentemente— que la consumación se materialice días después. Esto se ve claramente en muchos resultados de los ciberdelitos (a la espera de que se conecte la víctima).

d) Y la *propia consideración de la representación/descuido del autor* en ámbitos de organización, en los que la víctima organiza sus derechos de modo socialmente usual. *A sensu contrario*, si la conducta de la víctima es inusual, habrá concurrencia de culpas o *autopuesta* en peligro.

De otra parte, hemos visto la posibilidad de encuadrar los ciberdelitos en figuras que pueden *postergar* su resultado dañoso, porque se cir-

[278] Jakobs, Derecho penal… *cit.*, 25/64 a 25/70.

[279] Vehling, K. H., *Schriften zum Strafrecht und Strafprozeßrecht*, Frankfurt, Peter Lang, 1991, p. 147.

cunscriben en una dimensión atemporal y en un mismo espacio, y, es que, por regla general, puede suceder un segundo resultado tardío. En esta dinámica pueden aparecer *daños sobrevenidos*, *permanentes* y *otros resultados tardíos*. En los primeros se parte de una primera lesión no resuelta que, unida a otras circunstancias, causan de manera indirecta un segundo perjuicio; los daños permanentes se caracterizan por una lesión duradera que condiciona también, indirectamente, otra lesión que se produce con posterioridad; y los resultados tardíos son los que proceden de una conducta peligrosa que causa la lesión de una manera directa, pero sin que se manifieste hasta tiempo después. Hay que determinar si una conducta ha creado un riesgo —visto de manera penal— relevante, para producir la segunda lesión, más allá del tiempo transcurrido entre el primero y el segundo resultado, cuestión que afecta la dinámica de los ciberdelitos al tratarse de un mismo espacio con tiempos modificables, según lo explicado.

En lo que al objeto de nuestra investigación afecta, hemos de concretar si los ciberdelitos pueden suponer un daño sobrevenido, daño permanente o un resultado tardío. Aquí parece importante señalar el juicio de previsibilidad que algunos autores requieren,[280] o el riesgo típico causado. En nuestra opinión, y asentados los postulados anteriores, el ciberdelito se puede producir de forma espontánea, simultánea y con visos de continuidad, por lo que su resultado permanente, sobrevenido o tardío, depende de las características de cada una de éstas, siendo común dicha potencialidad.

La *dimensión temporal* como *forma* de la imputación objetiva se aprecia más acusadamente en los llamados *resultados tardíos*: ha de tenerse muy en cuenta la configuración temporal de la sociedad. Roxin[281] alega que en la lesión se consume el riesgo de otro proceso causal porque, el no considerarlo, sería obligar al autor a un deber de vigilancia permanente. Así, la diferencia entre aquellos daños causados, lenta, pero de manera continua, y otros en los que la enfermedad se detiene y años después causa la muerte súbitamente, es lo que le lleva a afirmar la imputación en los primeros perjuicios y reducirla sólo a las lesiones en los segundos. Su razonamiento se basa en la *determinación del fin de protección de la norma*: si la lesión que sobreviene no es de las que el fin de la norma no trata de evitar, menos aún en los casos de daños perma-

[280] Gómez Rivero, Ma., *La imputación de los resultados producidos a largo plazo: especial referencia a la problemática del SIDA*, Valencia, Tirant lo Blanch, 1998, pp. 52 y ss.

[281] Roxin, *op. cit.*, pp. 181-199

nentes. Jakobs, por su parte, lleva la imputación a la parte de la conducta del autor que ha transgredido el riesgo permitido, casos en los que se crea un riesgo penalmente relevante. De aquí que cuando la víctima obra bajo una situación desventajosa causada por el autor, se pueda seguir imputando el resultado.[282] Por su parte, Vásquez Shimajuko opina que "no cabe concebir como riesgo típico la potencialidad de una acción de causar consecuencias lesivas fuera del plazo de imputación objetiva de la conducta".[283] Alega, de manera acertada, que los criterios como el grado de riesgo o la forma en que se desenvuelve no sirven para establecer una regla de imputación objetiva, ni seguridad jurídica, en el límite temporal de la imputación del resultado.[284]

Un buen ejemplo de lo dicho es la diferenciación en el ámbito del ciberespacio de la imputación objetiva de los *delitos permanentes* y los *delitos de Estado*. En ambos se suscita la prolongación de la consumación, sin embargo, la cuestión trascendental para la imputación tardía del resultado es que el autor tenga la capacidad de prolongarla. En nuestra opinión, esta capacidad se incluiría tanto en los delitos permanentes como en los delitos de Estado o de pertenencia a organización,[285] por cuanto la capacidad de seguir perteneciendo pasa por la voluntad del sujeto, tanto dolosa o como imprudente —como veremos—, cuya trascendencia es la persistente comisión del tipo, por esto son delitos permanentes y de aquí la posibilidad de resultados tardíos derivados de dicha permanencia-permanente.[286]

Por ejemplo, en los delitos de sabotaje, distribución de pornografía infantil o estafas informáticas, puede suceder que una conducta no lesiva se torne muy destructiva con el tiempo, o una lesiva en otro resultado perjudicial. Entonces el tiempo es crucial para determinar el inicio de la ejecución y la consumación.[287]

---

[282] Jakobs, Derecho penal… *cit.*, 7/75 y ss.

[283] Vásquez Shimajuko, S., *La imputación de los resultados tardíos. Acerca de la dimensión temporal de la imputación objetiva*, Montevideo-Buenos Aires, B de F, 2010, p. 309.

[284] *Ibidem*, p. 357. De este modo, Vásquez Shimajuko encuentra, en la *prescripción de la* pena, el límite que la sociedad ha impuesto para el "proceso de superación social del pasado que ella trae consigo".

[285] Jakobs, Derecho penal… *cit.*, p. 32/28.

[286] Vásques Shimajuko, *op. cit.*, pp. 206-208

[287] Corcoy Bidasolo, *op. cit.*, pp. 29-30.

Asimismo, la *imprudencia* en el envío de contenido ilícito suscita problemas de imputación en ciertos delitos que sólo permiten la conducta dolosa, por ejemplo, en los delitos de descubrimiento y revelación de secretos, estafa o pornografía infantil. También se suscitan problemas de imputación cuando una misma acción produce indeterminados resultados lesivos a programas informáticos, cuentas bancarias o cuando se posibilita que un usuario vea el contenido pornográfico infantil pasado meses, incluso años.[288]

Esto es, la cibercriminalidad posibilita la *continuidad* delictiva y su *permanencia* en *tiempos modificables* en un mismo espacio (daños tardíos, sobrevenidos y delitos de Estado como la organización criminal/sistema de injusto).

6.4 El sistema de injusto y los injustos sistémicos de los ciberdelitos: autoría y participación, organización criminal y persona jurídica

La criminalización de las organizaciones se debe al auge masivo en los últimos tiempos de la criminalidad económica y de empresa, que se caracterizan por la intervención de varios sujetos, habitualmente especializados, cada uno con una aportación criminal adecuada al resultado o riesgo (*sentido*).

De aquí también que se pueda concluir que el *injusto sistémico* de la organización criminal constituye un *delito permanente* mientras exista la organización peligrosa.[289] El delito se consuma *de manera espontánea* (*autopoiesis*) por ser un *sistema de injusto*, y traslada el instante de la consumación hasta el fin de la organización, aun cuando dicha decisión haya sido imprudente (la constitución del sistema u organización no siempre es intencional, también, por ejemplo, el *obrar conjunto descuidado* en la coautoría).[290]

Una decisión criminal (dolosa) o en cuyo seno se cree un alto riesgo objetivo (imprudencia/comunidad de riesgo) puede constituir un injusto cuando se exterioriza. De este modo, cualquier *operación* realizada por

[288] *Ibidem*, p. 30.

[289] Bardavío Antón, *op. cit.*, pp. 814 y ss.

[290] Roxin, Claus, *Autoría y dominio del hecho en derecho penal*, Barcelona, Marcial Pons, 2000, p. 741.

una organización que pone en peligro la operatividad del sistema social se combate, de manera que se expulsa del mismo, siendo de este modo un dato más el dolo o la imprudencia: *es tratado como un peligro*. Y es que una organización es una *institución*,[291] lo cual ayuda a simplificar el problema de que *una organización criminal es una coautoría de mayor calado cuantitativo y cualitativo*.

A partir de estos planteamientos, la doctrina funcionalista ha formulado un modelo de imputación colectiva. Acerca del subsistema del derecho penal, Lampe[292] señaló que los *sistemas de injusto* son sistemas sociales, construcciones sociales con un *fin asocial*, cuya suma de individuos y operatividad posibilita la organización[293] mediante la comunicación interna y constante, al igual que sucede en otros tipos de sistemas sociales (*imputación colectiva*), precisamente porque cada sujeto aporta algo que por sí sólo sería ya no sólo inidóneo, sino imposible para el delito, pero, sumados todos, alcanzan significación y relevancia jurídica o, al menos, un peligro objetivo. Supone un *injusto directo* de la agrupación, asociación o de la entidad, distinta de la imputación de cada miembro por el delito en concreto que hayan comenzado a ejecutar o consumado.

Lo mismo cabe decir respecto al actual fundamento de responsabilidad penal de la *persona jurídica*, pues ésta misma no deja de ser una organización, un sistema. En este sentido, Gómez-Jara estima que puede fundamentarse la responsabilidad de la organización en que "la cultura empresarial tiene una determinada vigencia que puede cuestionar la vigencia del ordenamiento jurídico".[294] La culpabilidad individual y empresarial es funcionalmente equivalente en tres puntos: la cultura organizativa de la empresa contribuye a la vigencia de la norma y en su reverso

---

[291] Luhmann, Organización… *cit.*, p. 255.

[292] Lampe, *op. cit.*, pp. 97 y ss.

[293] Al respecto, Luhmann explicaba que la organización supone un modo particular de formar sistemas. Una propiedad de las organizaciones es que sus decisiones (*operaciones*) consisten en una sucesión de eventos, que guardan una clara relación en la operatividad de la organización que no permite dividirlos sin incurrir en una *paradoja*, por cuanto lo que antes sucede como operación absorbe la incertidumbre del futuro y lo establece como certidumbre, de manera que "instantes temporales desaparecen por sí mismos, aunque no se haga nada". Véase, Luhmann, N., *Poder*, México, Anthropos, 2005, pp. 25-26, 140 y 186.

[294] Gómez-Jara Díez, C., "Auto-organización empresarial y autorresponsabilidad empresarial. Hacia una verdadera responsabilidad penal de las personas jurídicas", *Revista Electrónica de Ciencia Penal y Criminología*, núm. 08-05, 2006, p. 15; y Gómez-Jara Díez, C., *La culpabilidad penal de la empresa*, Madrid-Barcelona, Marcial Pons, 2005, p. 75.

la defrauda.[295] Amén de ello, la responsabilidad de las organizaciones empresariales no se deriva de la actuación *estricto sensu* de las personas físicas ni de los órganos que la dirigen, sino de la *institucionalización de la autorresponsabilidad organizativa*[296] y, sobre todo, en nuestra opinión, por la producción de riesgos que se realizan a través de las *decisiones* con semejante sentido y resultado comunicativo.[297]

Entonces, dentro de esta forma de configurar el injusto, podemos señalar, por una parte, la organización delictiva en sí misma (coautoría)[298] como un *injusto simple*,[299] que, en muchos casos, genera un mayor injusto, justo por la seguridad y garantía de consumación delictiva, gracias a la aportación *ad hoc* de varios sujetos; y por otra, la organización criminal como *injusto constitutivo*, por ejemplo, la banda, asociación o la entidad con o sin personalidad jurídica,[300] cuyo fin es el delito como *delito de estatus*.[301]

---

[295] Gómez-Jara, Auto-organización… *cit.*, pp. 17-18.

[296] Gómez-Jara, La culpabilidad… *cit.*, pp. 91 y ss.

[297] Bardavío Antón, C., "Imputación y límites del riesgo en la responsabilidad penal de la persona jurídica: premisas y fundamentos de una 'auténtica' autorresponsabilidad", en Pere Simón Castellano y Alfredo Abadías Selma (coords.), *Mapa de riesgos penales y prevención del delito en la empresa*, Madrid, Wolters Kluver, 2020.

[298] El problema de la autoría y participación viene de la introducción, en los códigos penales, de una *degradación* de los conceptos de intervención, que han sido interpretados de manera tradicional como títulos de responsabilidad jurídica. En verdad, todos los intervinientes en el hecho típico comparten la responsabilidad, sin perjuicio de que cada uno realiza un *injusto propio*. Véase, Una teoría de la intervención delictiva, en Miguel Polaino-Orts (ed.), *El lado comunicativo y el lado silencioso del derecho penal. Expectativas normativas, intervención delictiva, derecho penal del enemigo*, España, Universidad de Sevilla, 2014, pp. 55-76.

[299] Polaino-Orts, M., *Derecho penal del enemigo. Fundamentos, potencial de sentido y límites de vigencia*, Barcelona, Bosch, 2009, p. 394

[300] *Idem*.

[301] Como bien precisa Silva Sánchez, existe una *institución antisocial* que se constituye, con independencia de los miembros, como *sistema de injusto* o *injusto sistémico autónomo*, que, incluso, hace posible el intercambio de sus partes, de sus sujetos (Lampe), lo que recuerda el argumento de Roxin sobre la *fungibilidad* o *intercambiabilidad* de los miembros en la autoría mediata de los aparatos organizados de poder. De esta manera, el injusto sistémico se configura en una parte objetiva, la reunión de varias personas, y, en una subjetiva, el fin aun indeterminado de delinquir. Al respecto, Polaino-Orts acierta en afirmar que "sólo la organización criminal constituye el sistema de injusto, y cada miembro de la organización es técnicamente la organización en sí"; asimismo, considera que "lo que aporta cada sujeto es *per se* algo naturalístico, es el entorno; sólo la organización criminal constituye el sistema de injusto, y —en este sentido— cada miembro de la organización es técnicamente la organización en sí", esto porque el sistema de injusto no de-

A juicio propio, y en contra del general criterio de que la autoría en la organización criminal precisa de un dolo en la "conformación", el fundamento de punibilidad reside en la especial *potencialidad de lesión* de la norma a través de un sistema, lo que nos hace concluir que la conjunción de personas que actúan u omiten, de manera imprudente (o comunidad de riesgo), sí crea la misma potencialidad objetiva de lesión (*inseguridad cognitiva*), también fundamentaría la punibilidad sin que se desvirtúe el fundamento, sino que adquiere todo el *sentido* de punibilidad de la organización.[302]

En nuestro ámbito de estudio, por ejemplo, sobre los casos especiales de los *intermediarios de la sociedad de la información*, Morales García[303] comenta que, en casos de doble rol de proveedor de contenidos y difusor de los mismos (como casos de infracción del deber de cuidado en la *tarea de selección de contenidos*), se aplicaría la limitación por la comisión imprudente o, en todo caso, por prohibición de regreso.

---

pende de la peligrosidad del aporte individual de cada sujeto en el delito-fin. Ya en su día, Wiener anticipaba este pensamiento en relación a que la parte del todo es más inteligente que el todo. De este modo, mediante la organización criminal, se *inhiben los factores de sentimiento de responsabilidad criminal* y se consigue una nueva forma de autoritarismo y/o peligrosidad objetiva para el sistema social y normativo. Véase, Silva Sánchez, J. Ma., "¿'Pertenencia' o 'intervención'? Del delito de 'pertenencia a una organización criminal' a la figura de la 'participación a través de la organización', en el delito", en Octavio de Toledo *et al.* (coords.), *Estudios en recuerdo del profesor Ruiz Antón*, Valencia, Tirant lo Blanch, 2003, p. 1075; Lampe, *op. cit.*, p. 111; Roxin, Autoría y dominio… *cit.*, pp. 269 y ss.; Polaino-Orts, Derecho penal… *cit.*, p. 71; Wiener, *op. cit.*; y Polaino-Orts, Imputación objetiva… *cit.*, p. 394

[302] Por ello, nos parecen correctas las palabras de Luhmann sobre la comunicación de *decisiones* en una organización, así como su relevancia en el sistema social. La organización tiene un *saber propio* y *ajeno al saber de cada individuo*, de dicho saber, determina la absorción de incertidumbre como certidumbre, es decir, peligrosidad objetiva, lo cual es bastante para atribuir responsabilidad a la organización. Véase, Luhmann, Organización… *cit.*, p. 222; y Poder… *cit.*, p. 140. De aquí viene que podamos considerar a una organización criminal a aquella que pone *en peligro* el sistema, aunque las aportaciones de los sujetos sean imprudentes, o, en el caso de la persona jurídica, cuando dicho defecto de organización se deba a la imprudencia, también al dolo en el defecto. Véase, Bardavío Antón, *op. cit.*, pp. 805-836.

[303] Morales García, O., "Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información", *Revista de Derecho y Proceso Penal*, núm. 5, 2001, pp. 139-167.

Por otra parte, Ortiz Márquez[304] distingue entre *proveedor de acceso* (alega la impunidad porque no tiene dominio del hecho), el *proveedor de enlace* (puede ejercitar cierto control sobre el enlace al que dirige al usuario en cuanto proveedores que incluyen en sus contenidos instrumentos de búsqueda: índices, motores de búsqueda, multibuscadores, registro de las páginas web) o como proveedores que incluyen directorios en sus contenidos (*links*, *banners*). He aquí la necesidad de la determinación del deber de control, es decir, la tipología de rol.

En este sentido, Ortiz Márquez considera que "la conducta realizada por el administrador de una página web al incluir en la misma un enlace a otra con contenido ilícito, en principio debe poder subsumirse en el tipo penal",[305] siempre y cuando tenga conocimiento o se representó dicha posibilidad como probable.

Al respecto, Corcoy Bidasolo recuerda la posibilidad de la *responsabilidad en cascada* del artículo 30 del Código Penal Español, sin embargo, concluye que los "ámbitos de responsabilidad en los que se basa el sistema de responsabilidad en cascada son diferentes, puesto que Internet se caracteriza por la ausencia de una organización jerárquica, sistema que está en el origen del art. 30 CP".[306] En su opinión, se puede trasladar el sistema de responsabilidad de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), al ámbito penal.[307]

De aquí que la problemática fundamental venga de los casos por *contenidos ajenos*. Corcoy Bidasolo comenta que, en principio, "debería-

[304] Ortiz Márquez, J. M., "Responsabilidad penal de los proveedores de enlaces", *Delito e informática: algunos aspectos*, Bilbao, Publicaciones de la Universidad de Deusto, 2007, pp. 260-264.

[305] *Ibidem*, pp. 265-266.

[306] Corcoy Bidasolo, *op. cit.*, p. 24.

[307] *Ibidem*, pp. 24-25. Al respecto, Corcoy Bidasolo comenta que "no puede pasarse por alto que, desde una perspectiva penal, en estos casos se trata realmente de una cooperación en un hecho ajeno. Sin embargo, siempre que se conozca la ilicitud puede hablarse de participación porque el delito no se ha consumado, ya que es necesaria la intervención del prestador de servicios para que esos datos puedan lesionar un bien jurídico [...] El problema surge respecto de la posibilidad de condenar a un partícipe desconociéndose quién es el autor, debido al principio de accesoriedad limitada de la participación. Ello explica la equiparación de las conductas de facilitamiento a las de ejecución directa en diversos delitos relacionados con las nuevas tecnologías". Así, también, Ortiz Márquez, *op. cit.*, pp. 269-271.

mos partir de la inexistencia de una obligación general de control por parte del proveedor en relación con los contenidos y actividades ajenas, al menos desde la perspectiva penal. No obstante […] la intervención penal debería reservarse para conductas dolosas de los prestadores de servicios".[308] Romeo Casabona[309] duda que se les pueda responsabilizar porque, aunque tienen posición de garante, no se cumple la equivalencia de la omisión y la acción en el aspecto subjetivo, el dolo. Y en opinión de Ortiz Márquez

> No cabe imputar a los motores de búsqueda y a los multibuscadores […] depende más de la destreza del autor de la página web mostrada a la hora de diseñar la misma que de la programación del robot realizada por el proveedor de enlace […] no tiene conocimiento de dicho contenido ni tiene el dominio del hecho […] Respecto a los proveedores que incluyen en sus contenidos directorios sí será posible imputar a los *link* y a los *banners* que dependen del administrador de la web y no de una empresa de gestión […] no será exigible en el supuesto en el que el contenido ilícito se halle oculto en la página".[310]

Y concluye que no puede aplicarse la comisión por omisión, salvo que asuman, de manera contractual, la posición de garante.

En nuestra opinión, en los casos citados de *proveedores de servicios* o *guardianes del ciberespacio* no sólo cabe la posibilidad de una responsabilidad por incumplimiento del deber de no dañar (*neminem laedere*), referido a cualquier rol común o por organización (deberes de relación o injerencia), sino, también, como explicábamos *supra*, la asunción de un deber puede generar *responsabilidad institucional*.

En lo institucional se crea una confianza con *intensidad equivalente a la comisión* que posibilita determinados contactos sociales que fundamentan la garantía, que puede venir de una *confianza que genera garantía* o de una *confianza que proporciona garantía*.[311] En la primera, se crea una confianza *ex novo*, que garantiza, por el receptor de ésta, un bien o el combate de un peligro, por ejemplo, el padre confía en que, cuando su hijo menor entra en una web de animaciones infantiles, no se le remita a contactos con pedófilos.

---

[308] *Ibidem*, p. 25.
[309] Romeo Casabona, *op. cit.*, pp. 21-22
[310] Ortiz Márquez, *op. cit.*, pp. 274-275.
[311] Jakobs, Derecho penal… *cit.*, pp. 29/67 y ss.

En la segunda, ya existe un deber de garante, en el que se concreta sólo el sujeto competente, según el ámbito de organización, no por su comportamiento, sino cuando entra en un determinado ámbito de organización; en este caso, por ejemplo, según el *plan del servicio* contratado. En tal sentido, ha de matizarse, en contra de lo expuesto por otros, que una conducta fortuita no cabe en el artículo 11 del CP español, por la sencilla razón de que éste pena la infracción de un deber, no omisiones simples, pues, de lo contrario, se vulneraría el artículo 6o. del CP, sin embargo, la acción precedente sí puede ser fortuita (o imprudente) y, a la postre, también entrar en el radio de acción del deber institucional (deber de evitar el resultado), por ejemplo, en el incumplimiento de controles,[312] porque aquí el fundamento de punibilidad reside en el hacer precedente.[313]

6.5 Conclusiones

Primera. La teoría de sistemas permite comprender que el *ciberespacio* es un nuevo *medio de comunicación* en el que se protege, de manera penal, ciertas comunicaciones que se producen ahí, sin perjuicio de injustos diferenciados. El ciberespacio posibilita hacer posible lo imposible, en concreto, nuevas formas criminales en un *mismo espacio*, pero con *tiempos modificables*, lo que posibilita la *simultaneidad* de los delitos, la potencialidad de la continuidad y daños tardíos, sobrevenidos, permanentes y/o delitos de Estado (organización criminal/persona jurídica: sistema de injusto).

Segunda. El ciberespacio transforma las tradicionales instituciones de la teoría del delito (acción, tipicidad, antijuricidad y culpabilidad, acto preparatorio/tentativa/consumación, y la autoría y participación), pero pueden adquirir coherencia mediante la teoría de sistemas y el funcionalismo normativo con la *autodescripción* de la *imputación objetiva*.

Tercera. Mediante la aplicación de una moderna teoría de la imputación objetiva, basada en la teoría de sistemas sociales, se puede explicar (*reflexividad* de la imputación) el fundamento de punibilidad de los delitos cometidos en el *espacio (-ciber)*. La imputación objetiva es una autodescripción del sistema penal, mediante la cual se transforma (hete-

[312] Mata y Martín, R. M., "Perspectivas sobre la protección penal del software", en Carlos María Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006, p. 230.

[313] Jakobs, Derecho penal… *cit.*, pp. 29/39 y ss.

rorreferencia) su entorno (espacio, tiempo, confianza, riesgos, roles, autonomía, controlabilidad/evitabilidad, querer/descuido, organización/institución, etcétera) y lo traduce a su propia referencia (autorreferencia), en *sentido* diferenciable: punible/no punible.

Cuarta. El ciberespacio propicia la diferenciación entre *sistemas de injusto* e *injustos sistémicos*. Los primeros son sistemas objetivamente peligrosos para la libre comunicación en dicho espacio, por ejemplo, los delitos de Estado (organización criminal), los delitos de la persona jurídica y la propia configuración de un sistema virtual de peligro objetivo. Los segundos, como resultado concreto (preparación tentativa, consumación) sobre bienes jurídicos. En ambos casos, el dolo y la imprudencia son datos que, exteriorizados (físicos), son susceptibles de fundamentar una imputación en relación al contexto.

Quinta. La *asunción de un deber* en el ciberespacio, al igual que en el espacio físico, puede generar no sólo una responsabilidad por organización, sino una *confianza especial* en *deberes institucionales*, con trascendencia en la responsabilidad penal, en la omisión del concepto de autor, según las circunstancias del contexto: capacidad de evitar el resultado.

Bibliografía

Adler, Freda, Gerhard O. Mueller y William Laufer, *Criminology and the criminal justice system*, 4a. ed., New York, McGraw Hill, 2001.

Alonso García, J., *Derecho penal y redes sociales*, Madrid, Aranzadi, 2015.

Ambos, K., "Responsabilidad penal internacional en el ciberespacio", en Fernando Velásquez *et al.* (comps.), *Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código* Penal, Bogotá, Universidad Sergio Arboleda, 2016.

Asencio-Guillén, A., y J. Navío-Marco, "El Ciberespacio como sistema y entorno social: una propuesta teórica a partir de Niklas Luhmann", *Communication and Society*, núm. 31, 2018.

Ashby, W. R., *An introduction to cybernetics*, London, Chapman & Hall, 1956.

Bardavío Antón, C., "Ciberdelitos: evolución hacia un derecho penal funcional incorrectamente dogmatizado", en Miguel Bustos Rubio y Alfredo Abadías Selma (dirs.), *Una década de reformas penales:*

análisis de diez años de cambios en el Código Penal (2010-2020), Barcelona, Bosch, 2020.

_____, "Imputación y límites del riesgo en la responsabilidad penal de la persona jurídica: premisas y fundamentos de una 'auténtica' autorresponsabilidad", en Pere Simón Castellano y Alfredo Abadías Selma (coords.), *Mapa de riesgos penales y prevención del delito en la empresa*, Madrid, Wolters Kluver, 2020.

_____, *Las sectas en derecho penal: estudio dogmático de los delitos sectarios*, Barcelona, Bosch, 2018.

Barrio Andrés, Moisés, *Ciberdelitos: amenazas criminales del ciberespacio. Adaptado reforma Código Penal 2015*, Madrid, Reus, 2017.

Bertalanffy, L., *Teoría general de los sistemas: Fundamentos, desarrollo, aplicaciones*. México, FCE, 1989.

Bleckmann, F., "Derecho penal y teoría de sistemas", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y Derecho penal: Fundamentos y posibilidades de aplicación*, Granada, Comares, 2005.

Cancio Meliá, M., *Conducta de la víctima e imputación objetiva en derecho penal. Estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas*, 2a. ed., Barcelona, Bosch, 2001.

Caro John, J. A., "Derecho penal del enemigo: garantía estatal de una 'libertad real' del ciudadano. Una glosa a Miguel Polaino-Orts", *Cuadernos de Derecho Judicial*, núm. 91, 2007.

_____, *La imputación objetiva en la participación delictiva*, Lima, Grijley, 2009.

Clough, J., *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010.

Corcoy Bidasolo, *Delitos de peligro y protección de bienes jurídico-penales supraindividuales: nuevas formas de delincuencia y reinterpretación de tipos penales clásicos*, Valencia, Tirant lo Blanch, 1999.

_____, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Eguzkilore*, núm. 21, 2007.

De la Cuesta Arzamendi, J. L., y Pérez Machío, A. I., "Ciberdelincuentes y cibervíctimas", en José Luis de la Cuesta Arzamendi (dir.) y Norberto Javier de la Mata Barranco (coord.), *Derecho penal informático*, Madrid, Civitas-Thomson Reuters, 2010.

_____, y C. San Juan Guillén, "La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad" en José Luis de la Cuesta Arzamendi (dir.) y Norberto Javier De la Mata Barranco (coord.), *Derecho penal informático*, Madrid, Civitas-Thomson Reuters, 2010.

De la Mata Barranco, N. J., y A. I. Pérez Machío, "La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española", en José Luis de la Cuesta Arzamendi (dir.) y Norberto Javier de la Mata Barranco (coord.), *Derecho penal informático*, Madrid, Civitas-Thomson Reuters, 2010.

Fernández Teruelo, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, Madrid, Constitutio Criminalis Carolina, 2007.

Foerster, H., *Las semillas de la cibernética. Obras escogidas*, Barcelona, Gedisa, 1991.

Gibson, W., *Neuromancer*, New York, Ace Books, 1984.

Gómez-Jara Díez, C., "Auto-organización empresarial y autorresponsabilidad empresarial. Hacia una verdadera responsabilidad penal de las personas jurídicas", *Revista Electrónica de Ciencia Penal y Criminología*, núm. 08-05, 2006.

_____, *La culpabilidad penal de la empresa*, Madrid-Barcelona, Marcial Pons, 2005.

_____, "Teoría de sistemas y derecho penal: culpabilidad y pena en una teoría constructivista del derecho penal", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Granada, Comares, 2005.

Gómez Rivero, Ma., *La imputación de los resultados producidos a largo plazo: especial referencia a la problemática del SIDA*, Valencia, Tirant lo Blanch, 1998.

González Rus, J. J., "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáti-

cos", *Revista de la Facultad de Derecho de la Universidad Complutense*, núm. 12, 1986.

_____, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", *Delito e informática: algunos aspectos*, Bilbao, Publicaciones de la Universidad de Deusto, 2007.

Herrera Moreno, M., "El fraude informático en el derecho penal español", *Actualidad Penal*, núm. 39, 2001.

Hruschka, J., *Strafrecht nach logisch-analytischer methode*, 2a. ed., Berlín-Boston, De Gruyter, 1988.

Jakobs, G., "Derecho penal del ciudadano y derecho penal del enemigo", en Günther Jakobs y Manuel Cancio Meliá, *Derecho penal del enemigo*, Madrid, Thomson-Civitas, 2003.

_____, *Derecho penal. Parte general. Fundamentos y teoría de la imputación*, Madrid, Marcial Pons, 1997.

_____, *Estudios de derecho penal*, Madrid, Civitas, 1997.

_____, *La imputación objetiva en derecho penal*, Madrid, Civitas, 1996.

_____, "La imputación jurídico-penal y las condiciones de vigencia de la norma", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Granada, Comares, 2005.

_____, "Sobre la teoría de la pena", *Bases para una teoría funcional del derecho penal*, Lima, Palestra Editores, 2000.

_____, Una teoría de la intervención delictiva, en Miguel Polaino-Orts (ed.), *El lado comunicativo y el lado silencioso del derecho penal. Expectativas normativas, intervención delictiva, derecho penal del enemigo*, España, Universidad de Sevilla, 2014.

Lampe, E. J., Injusto del sistema y sistemas de injusto, en Carlos Gómez-Jara Díez *et al.* (eds.), *La dogmática jurídico-penal entre la ontología social y el funcionalismo*, Lima, Grijley, 2003.

Lesch, H. H., *Das problem der sukzessiven beihilfe*, Frankfurt-New York, P. Lang, 1992.

Luhmann, Niklas, "El derecho como sistema social", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Granada, Comares, 2005.

_____, *El derecho de la sociedad*, 2a. ed., México, Universidad Iberoamericana/Biblioteca Francisco Xavier Clavigero/Herder, 2005.

_____, *La confianza*, México, Anthropos, 2005.

_____, *La moral de la sociedad*, Madrid, Trotta, 2013.

_____, *La sociedad de la sociedad*, México, Herder, 2007.

_____, *La realidad de los medios de masas*, México, Anthropos, 2007.

_____, *Organización y decisión*. México, Herder, 2010.

_____, *Poder*, México, Anthropos, 2005.

_____, *Sistemas sociales. Lineamientos para una teoría general*, 2a. ed., México, Anthropos, 1998.

Maraver Gómez, M., *El principio de confianza en derecho penal. Un estudio sobre la aplicación del principio de autorresponsabilidad en la teoría de la imputación objetiva*, Madrid, Civitas, 2009.

Mata y Martín, R. M., *Delincuencia informática y derecho penal*, Madrid, Edisofer, 2001.

_____, "Perspectivas sobre la protección penal del software", en Carlos María Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006.

Maturana H., y Varela F., *De máquinas y seres vivos. Autopoiesis: la organización de lo vivo*, 5a. ed., Chile, Universitaria, 1988.

Miró Llinares, F., *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012.

_____, "La cibercriminalidad 2.0: falacias y realidades", en Fernando Velásquez *et al.* (comps.), *Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal*, Bogotá, Universidad Sergio Arboleda, 2016.

Morales García, O., "Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información", *Revista de Derecho y Proceso Penal*, núm. 5, 2001.

Morales Prats, F., "Internet: riesgos para la intimidad", *Cuadernos de Derecho Judicial*, núm. 10, 2001.

Morón Lerma, E., *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, 2a. ed., Pamplona, Aranzadi, 2002.

Müssig, B., "Aspectos teórico-jurídicos y teórico-sociales de la imputación objetiva en derecho penal. Puntos de partida para una sistematización", en Carlos Gómez-Jara Díez (ed.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Granada, Comares, 2005.

Ortiz Márquez, J. M., "Responsabilidad penal de los proveedores de enlaces", *Delito e informática: algunos aspectos*, Bilbao, Publicaciones de la Universidad de Deusto, 2007.

Piña Rochefort, J. I., *Rol social y sistema de imputación. Una aproximación sociológica a la función del derecho penal*, Barcelona, Bosch, 2005.

Polaino Navarrete, M., *Acción, omisión y sujetos en la teoría del delito. De la posición de garante a la responsabilidad penal de las personas jurídicas*. Perú, Grijley, 2009.

_____, *Lecciones de derecho penal. Parte general*, 2a. ed., Madrid, Tecnos, 2016, t. II.

Polaino-Orts, M., *Derecho penal del enemigo. Fundamentos, potencial de sentido y límites de vigencia*, Barcelona, Bosch, 2009.

_____, "Imputación objetiva: esencia y significado", *Imputación objetiva e imputación subjetiva en derecho penal*, Perú, Grijley, 2009.

Posada Maya, R., "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", *Revista Nuevo Foro Penal*, núm. 13, 88, enero-junio, 2017.

_____, "¿Puede ser el cibercrimen un delito organizado y transnacional?", en Juan Carlos Rodas Montoya (ed.), *Temas de derecho penal*

económico y patrimonial, Medellín, Universidad Pontificia Bolivariana, 2018.

Requena Juliani, J., *Intercambiabilidad de acción y omisión en los delitos de dominio: posición de garante e imputación objetiva*, Madrid, Dykinson, 2010.

Romeo Casabona, C. Ma., *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006.

_____, *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información*, Madrid, Fundesco, 1988.

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

Roxin, Claus, *Autoría y dominio del hecho en derecho penal*, Barcelona, Marcial Pons, 2000.

_____, *Derecho penal, Parte general. Fundamentos. La estructura de la teoría del delito*, Madrid, Civitas, 1997, t. I.

_____, *Problemas básicos de derecho penal*, Madrid, Reus, 1976.

Sánchez-Vera, J., *Delito de infracción de deber y participación delictiva*, Barcelona, Marcial Pons, 2002.

Sieber, U., *Computerkriminalität und Strafrecht*, Berlín, Heymann, 1977.

Silva Sánchez, J. Ma., "¿'Pertenencia' o 'intervención'? Del delito de 'pertenencia a una organización criminal' a la figura de la 'participación a través de la organización', en el delito", en Octavio de Toledo *et al.* (coords.), *Estudios en recuerdo del profesor Ruiz Antón*, Valencia, Tirant lo Blanch, 2003.

Tiedemann, K., "Criminalidad mediante computadoras", *Nuevo Foro Penal*, Bogotá, núm. 30, octubre-diciembre, 1985.

_____, *Poder económico y delito*, Barcelona, Ariel, 1985.

Vásquez Shimajuko, S., *La imputación de los resultados tardíos. Acerca de la dimensión temporal de la imputación objetiva*, Montevideo-Buenos Aires, B de F, 2010.

Vehling, K. H., *Schriften zum Strafrecht und Strafprozeßrecht*, Frankfurt, Peter Lang, 1991.

Velásquez, F., "Criminalidad informática y derecho penal: Una reflexión sobre los desarrollos legales colombianos", *Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal*, Bogotá, Universidad Sergio Arboleda, 2016.

Welzel, H., *Derecho penal alemán. Parte general*, 2a. ed., Santiago de Chile, Jurídica de Chile, 1976.

Wiener, N., *Cybernetics: or control and communication in the animal and the machine*, Cambridge-Massachusetts, The Massachusetts Institute of Technology, 1948.

Fuentes de consulta

Aguirre Romero, J. Ma., "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI", *Espéculo, Revista de Estudios Literarios*, Universidad Complutense de Madrid, [en línea], núm. 27, julio-octubre 2004, Formato html, Disponible en: *http://www.ucm.es/info/especulo/numero27/cibercom.html*

Miró Llinares, F., "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13, 07, 2011, Formato pdf, Disponible en: *http://criminet.ugr.es/recpc/13/recpc13-07.pdf*