Capítulo VI

Algoritmos y big data *en la responsabilidad penal: el reto de la cibercriminalidad en el Derecho Penal*

Jacinto Pérez-Arias

Sumario: 1. Introducción – 2. La informática y el Derecho Penal: la inteligencia artificial – 3. Límites normativos – 4. Problemas procesales ¿*vs*? problemas penales – 5. Sujeto activo, resultado y culpabilidad: juicio de probabilidad estadística – 6. Conclusión – 7. Bibliografía

1. *Introducción*

Es difícil encarar, en un trabajo de esta naturaleza, un problema con tantas aristas como la cibercriminalidad. El derecho penal, anclado en sus principios clásicos, necesita responder a nuevos retos que, a su vez, pueden exigir de él nuevos principios (si lo que se pretende es idear una respuesta global y satisfactoria al problema). Mientras tanto eso llegue, e inspirándonos en G. Radbruch[1], debemos ver cómo mejorar el derecho penal, hasta tener algo mejor que el derecho penal.

Ante todo, debemos valorar si la cibercriminalidad constituye un problema jurídico-penal o no y, si lo es, si tiene solución jurídico-penal o no. Y decimos un problema jurídico penal, pues no debemos confundir el problema sustantivo (material) con las dificultades procesales que puedan surgir en la investigación y enjuiciamiento de los delitos derivados de, o con causa en, la cibercriminalidad.

Como señala J.M. Peris Riera[2], ser conscientes de los grandes riesgos que entrañaría una aplicación mecánica de los avances en neurociencia y en inteligencia artificial, no debe comportar un abandono de esta fuente de conocimiento; no debe suponer en absoluto un aislamiento por parte del

[1] G. Radbruch, *Einführung in die Rechtswissenschaft*, Quelle & Meyer, Stuttgart, 1929, p. 11.
[2] J. Peris Riera, *Inteligencia Artificial y Neurociencias: Avances Del Derecho Penal Contemporáneo*, en esta obra, p. 3

derecho penal de los nuevos avances técnicos en estas materias. Más bien deben ser tenidos en cuenta para mejorar la técnica procesal y judicial, pero teniendo presente que todo lo técnicamente posible no tiene por qué ser jurídicamente admitido.

La multidisciplinar temática de la ciberdelincuencia afecta, también, a la criminología (la llamada cibercriminología, en término acuñado por Jaishankar[3]), donde se están haciendo avances importantes en la materia, sobre todo, en lo relacionado con el perfil del ciberdelincuente; y ello, aunque la propia ONU concluyera, en su XIII Congreso sobre Prevención del Delito y Justicia Penal de 2015, que no había un perfil estándar del ciberdelincuente[4]. No obstante, y como se ha matizado, esta poco halagüeña intuición nace de la propia naturaleza técnica, pero igualmente dinámica y constantemente innovadora de los denominados ciberdelitos: por un lado, su perpetración requiere de unos conocimientos cualificados en materia informática; por el otro, su versatilidad y el avance en la disponibilidad de las nuevas Tecnologías de la Información y la Comunicación (TIC´s), hacen posible que, al igual que los interfaz informáticos necesarios para su comisión, la realización de actos delictivos a través de medios telemáticos se encuentre, cada vez más frecuentemente, al alcance de cualquiera que sepa manejar –aunque sea de forma rudimentaria o a nivel 'usuario'- un dispositivo. Más aún, es posible que las cualificaciones técnicas poseídas por algunos sujetos sirvan de puerta de entrada a otros con conocimientos mucho menores, que se aprovechan del trabajo ya realizado por los primeros para cometer hechos delictivos a través de medios informáticos (S. Cámara Arroyo[5]).

Como se señala por J.M. Tamarit Sumalla[6], la evolución hacia la sociedad de la información ha supuesto una transformación profunda de las relaciones sociales, y uno de los efectos de dicho proceso ha sido la transformación de la delincuencia. Buen ejemplo de ello es la evolución de la delincuencia juvenil, que siempre ha sido un fenómeno particularmente

[3] Considerado el fundador de esta rama de la criminología, Jaishankar entiende la cibercriminología como una materia multidisciplinar que abarca diversos campos, tales como la Criminología, la Victimología, la Sociología, la Ciencia de Internet y las Ciencias de la computación (así lo recuerda S. Cámara Arroyo. *Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente*, en «Derecho y Cambio Social», Núm. 60, Abril-junio 2020, pp. 471-472.

[4] Informe del 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, A/CONF.222/17. 29 de abril de 2015.

[5] Cámara Arroyo. *Estudios criminológicos contemporáneos*, cit., pp. 482.

[6] J.M. Tamarit Sumalla. *Ciberdelincuencia y cibervictimización*, en «Revista de los Estudios de Derecho y Ciencia Política», n.º 22, Junio, 2016, p. 30.

estudiado por la criminología y que puede funcionar como un punto de observación de las tendencias, de anticipación del futuro y de experimentación de nuevas formas de justicia y de tratamiento de la criminalidad.

En su día señalamos (J. Pérez-Arias[7]), que el sucesivo incremento de los inventos tecnológicos, y el casi preocupante (ab)uso de las nuevas tecnologías (hasta para las cosas más básicas), ha convertido lo cibernético en un nuevo mundo, con reglas nuevas y riesgos y/o peligros desconocidos. Solo ha de pensarse en los datos personales que cada individuo entrega a la red, y en la posibilidad de uso, por terceros anónimos, de tales datos, incluso sin el conocimiento directo ni indirecto de la víctima. Es evidente que este nuevo mundo (esa nueva modernidad a la que se refería U. Beck[8]) arroja un cúmulo de nuevos riesgos, que merecen, al menos teóricamente -no necesariamente en términos legislativos- un estudio y tratamiento especializado, que tenga en cuenta todas las variables que confluyen en este, cada vez más expandido, fenómeno social de redes (o, dicho de otro modo, en esta nueva sociedad cibernética, que se impone sobre la ya denominada sociedad tradicional o antigua).

2. *La informática y el Derecho Penal: la inteligencia artificial*

El Derecho Penal no queda extramuros de todo este nuevo mundo[9]. Por ello, se ha afirmado que la revolución social y técnica que implican las nuevas tecnologías traen consigo también efectos en lo que al Derecho penal respecta (R.M. Mata y Martín[10]).

La cibercriminalidad, como fenómeno técnico, exigiría una valoración exhaustiva de todas y cada una de las categorías de la teoría jurídica del delito[11], por lo que podemos extraer ya una primera conclusión: estamos ante

[7] J. Pérez-Arias, *Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal*, en «Revista internacional de doctrina y jurisprudencia», Volumen 26 (diciembre 2021), Universidad de Almería, p. 182.

[8] U. Beck. *Sociedad de riesgo*. *Hacia una nueva modernidad*, Paidós, Barcelona-Buenos Aires-México, 2002.

[9] Pérez-Arias, *Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal*, cit., p. 176.

[10] R.M. Mata y Martín, *Criminalidad informática: una introducción al cibercrimen*, en «Actualidad Penal», 37, Semana del 6 al 12 Oct. 2003, Ref. XXXVI, tomo 3, p. 935.

[11] Como señala Peris Riera, la responsabilidad penal que pueda nacer de condicionantes basados en inteligencia artificial debería ser individualizada a partir de los criterios generales inherentes a la teoría general del delito (Peris Riera, *Inteligencia Artificial y*

una cuestión compleja[12]. Así lo entiende también A. Giraldi[13], para quien la inteligencia artificial se ha desarrollado hasta llegar a influir no sólo en la realidad social, sino también en las instituciones básicas del Derecho penal.

Ahora bien, su complejidad no puede confundirse ni con su desconocimiento (todo lo desconocido parece complejo), ni con el incómodo y habitual uso indiscriminado de términos ingleses (siempre de poca ayuda conceptual). Cuando lejos de divulgar se pretende construir una teoría válida, los anglicismos pierden importancia. Solo cuentan las bases teóricas y su respaldo dogmático. Y ahí es donde empieza el verdadero problema. Es hora, pues, de que la doctrina comience a construir el necesario *andamio para las ideas*, en palabras tan expresivas de A. Muñoz Alonso[14].

Se señala por F. Miró Linares[15], y estamos por completo de acuerdo, que algunos términos generan una expectativa superior a su propia realidad, y cuando se compara lo que expresa el concepto con la concreción del mismo en la práctica, llega la pequeña o gran decepción.

Cada vez que se impone una tendencia, rápidamente surgen las dudas de si existe una adecuada regulación penal y un adecuado tratamiento teórico. Pasó con la lucha por el medioambiente, pasó con la responsabilidad penal de las personas jurídicas y obviamente tenía que pasar con la cibercriminalidad.

A nuestro entender, la cibercriminalidad comparte caracteres de estas dos temáticas penales: Del medio ambiente comparte su peligrosidad y la eterna cuestión de si estamos o no admitiendo conductas generadoras de riesgos no tolerables, lo que nos llevará a la ardua cuestión del peligro relevante; y de las personas jurídicas participa de la singularidad de un sujeto penal altamente discutible (en nuestro caso, la inteligencia artificial) y con clara falta de sintonía con el concepto clásico de autor.

Una vez surge la tendencia, el problema se pone de moda y alguna literatura jurídica o criminológica, y los medios divulgativos empiezan a crear teorías, en la mayoría de los casos sin base firme ni normativa. Estas

Neurociencias: Avances Del Derecho Penal Contemporáneo, en esta misma obra, p. 3).

[12] Como afirma L. Hernández Díaz, la primera dificultad a la hora de afrontar el análisis de los delitos informáticos es su conceptualización (L. Hernández Díaz, *El delito informático*, en «EGUZKILORE. Cuaderno del Instituto Vasco de Criminología», Número 23. San Sebastián, diciembre 2009, p. 228.

[13] A. Giraldi, *Deshumanizando la culpabilidad: los sistemas inanimados en la teoría del delito*, en esta obra.

[14] A. Muñoz Alonso, *Andamios para las ideas*. Colección Aula de ideas, volumen 1, Aula, Madrid. 1952.

[15] F. Miró Linares, *El sistema penal ante la inteligencia artificial: Actitudes, usos, retos*, en *Cibercrimen III* (Dir. D. Dupuy/ J.G. Corvalán), B de f, Buenos Aires, 2020, p. 81.

teorías chocan con la realidad, y terminan generando folios de disertaciones (sin hablar de horas de televisión), sin apenas contar con una regulación cierta, seria y sistemática. Si tres palabras rectificadoras del legislador convierten bibliotecas enteras en basura (J. Kichmann[16]), podemos imaginar qué es lo que ocurre cuando la literatura científica inicia su andadura de razón práctica mucho antes de que el legislador haya mostrado su derrotero político criminal.

Los dos principales problemas, a nuestro entender, son, de un lado, de sujeto (con todo lo que ello comporta desde perspectivas de capacidad consciente) y, de otro, de conducta. Pero adviértase que hablo de sujeto y no de autor, porque para admitir la autoría antes se ha debido depurar si existe o no un sujeto con aptitud para realizar hechos por algún concepto y con capacidad de culpabilidad. No se puede hablar en directo de autor, porque el autor no es una premisa teórica, sino una consecuencia práctica[17]. Hablar de autoría, sin tener claro esto, nos llevaría nuevamente a la creación artificial de un sujeto difícil de digerir, como ocurrió, mediante la reforma del código penal español operada a través de la Ley Orgánica 5/2010, con la persona jurídica.

Con todo lo relevante y novedoso que pudiera parece la temática, el problema de la cibercriminalidad no es un absoluto desconocido para el Derecho. Aparte de la normativa europea, que ha sido la gran precursora de toda la regulación española en la materia, a nivel dogmático encontramos a C.M. Romeo Casabona[18], que a finales de la década de los 80, del siglo pasado, hablaba ya de la relación entre el poder informático y seguridad jurídica.

Sin embargo, lo informático ha dado paso al ciberespacio, entendido como aquella realidad espacio-virtual, que no tiene una localización física y que abarca los sistemas de información y comunicación contenidos en la Red (S. Morán Blanco[19]). Hoy no solo preocupa el acceso ilícito a un terminal, que también, sino la existencia de un espacio virtual dinámico, en el que se genera biografía vital de cada uno, personal y con contenido y trascendencia económica. ¿Somos conocedores de que nuestra vida está expuesta a un espacio sin control y que los ataques pueden venir incluso

[16] Frase que afirmó en una conferencia en la sociedad jurídica de Berlín celebrada en 1847, y publicada al año siguiente.

[17] Sin olvidar su trascendencia teórica.

[18] C.M. Romeo Casabona, *Poder informático y seguridad jurídica. la función tutelar del derecho penal ante las nuevas tecnologías de la información*, Fundesco, Madrid, 1988, pp. 42 y ss.

[19] S. Morán Blanco. *La ciberseguridad y el uso de las tecnologías de la información y la comunicación (tic) por el terrorismo*, en «Revista Española de Derecho Internacional», vol. 69/2, julio-diciembre 2017, p. 197.

sin tocar, en el momento de la acción, nuestro ordenador, nuestra tableta o nuestro móvil?: Esa es la otra cara del mundo de los datos (de la Big Data) y de la inteligencia artificial[20].

Y todavía existe más riesgo desde que esas aplicaciones -tan útiles[21]- tienen capacidad para activar micrófonos, cámaras y deambulan por nuestros datos más íntimos porque nosotros lo hemos consentido. Esto genera también un problema en la víctima, dado que, desde el punto de vista penal, en este tipo de delitos, la víctima es crucial, en la mayoría de los casos, para la posible comisión del delito. De hecho, lo que permitirá activar la conducta en su contra -insistimos que, en la mayoría de los casos, no en todos- será la 'confianza' que deposita en algo que tiene constantemente en sus propias manos (el teléfono móvil, por ejemplo). Nadie suele pensar que su intimidad está en riesgo. Pero lo relevante y peligroso de ese artefacto, como sabemos, no está entre las manos, está en la red, en esa 'nube'. El peligro, por tanto, no es lo tangible (que es lo que genera falsa confianza), sino lo intangible (esa autopista de datos, que encuentra su entrada y salida en el artefacto que uno tiene entre sus manos).

Como afirma la SAP de Barcelona[22], la modalidad ciberdelictiva más habitual es la de los fraudes [engaños] en internet, que se ha convertido, con sus 192.375 casos en el 88,1% de total de los ciberdelitos. Coincidimos con J.R. Agustina[23], cuando afirma que la relación entre ofensor y víctima, mediada por 'máscaras virtuales', facilita al ofensor el recurso a apariencias engañosas, técnicas de camuflaje y de manipulación, y potencian en la víctima una serie de déficits cognitivo-conductuales que incrementan notablemente los riesgos de victimización.

A nivel conceptual, la inteligencia artificial es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de

[20] Término acuñado por John McCarthy, en el año 1956 (véase para mayor profundidad M. Cumbreras, P. López, *¿Es necesario un marco ético para guiar el desarrollo y uso de la inteligencia artificial en las organizaciones?*, en *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0* (Coord. M.J. Cruz Blanca/I. Lledó Benito), Dykinson, Madrid. 2021. p. 450.

[21] Utilidad no solo en lo personal, pues no debemos olvidar el evidente progreso que se produce en la ciencia forense, gracias a esta tecnología.

[22] SAP Barcelona de 9 de julio de 2020 (ECLI:ES:APB:2020:7301), p. 3

[23] J.R. Agustina. *Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización*, en «Cuadernos de política criminal», 136, Mayo 2022, p. 159.

planear[24]. Esta habilidad, como señala R. Kurzweil[25] y recuerdan S. Russel/P. Norvig[26], es el arte de desarrollar máquinas con capacidad para realizar funciones que cuando son realizadas por personas requieren de inteligencia. Sin embargo, así como la inteligencia humana está limitada por el nacimiento, la inteligencia artificial no encuentra más límites que el estado de desarrollo de la ciencia; de tal forma que cuanto más avance el conocimiento sobre el procesamiento informático, más capacidad de desarrollo tendrá la máquina con inteligencia artificial. O, dicho con otras palabras, la inteligencia artificial es una fuente de riesgos que será mayor conforme el sistema inteligente adquiera la capacidad de reproducir la forma de funcionamiento del cerebro humano y goce de mayor autonomía en la toma de decisiones (J.M. Palma Herrera[27]).

Y eso es así, porque la máquina solo requiere el enfoque racional, que implica una combinación de matemáticas e ingeniería[28]. De hecho, el gran problema que genera actualmente la big data es que estamos en presencia de un número ingente de datos cuya administración y gestión no puede realizarse a través de las tradicionales bases de datos, sino a través de esa nueva tecnología en que consiste la inteligencia artificial[29].

No puede extrañar, pues, que la actual sociedad esté por completo digitalizada. La vida actual ha cedido por completo al avance de una técnica que tiene capacidad para abarcarlo prácticamente todo, y es lógico que en el mundo personal y en el mundo empresarial se quieran usar recursos que abaratan costes e incrementan resultados/beneficios.

La desinformación social es la clave que dificulta todo. Una desinformación que se observa en la facilidad de crear (y creer) hechos inexistentes (*fake news*), en la extrema confianza y 'falsa' necesidad de las redes sociales y en el comercio electrónico. Es más, esa desinformación es la gran aliada de la ciberdelincuencia, pues es la que explica el recelo de los ciudadanos frente a las instituciones (con potestad legislativa), cuando éstas quieren regular y poner límites normativos al ciberespacio; unos límites que

[24] Definición obtenida de <https://www.europarl.europa.eu>

[25] R. Kurzweil. *The Age of Intelligent Machines*, MIT Press, Cambridge, 1990.

[26] S. Russel, P. Norvig, *Inteligencia artificial. Un enfoque moderno*, Pearson, Madrid. 2008, p. 2.

[27] J.M. Palma Herrera. *Inteligencia artificial y neurociencia. Algunas reflexiones sobre las aportaciones que pueden hacer al Derecho Penal*, en esta obra.

[28] Russel, Norvig. *Inteligencia artificial. Un enfoque moderno*, cit., p. 2.

[29] Para mayor profundidad, vid C. Maté Jiménez. *Big data. Un nuevo paradigma de análisis de datos*. anales de mecánica y electricidad, en <https://www.iit.comillas.edu>, noviembre-diciembre 2014, pp. 10-16.

se perciben por la sociedad como una limitación de derechos y no como una barrera de protección. Y lo más preocupante es que, apenas están saliendo a la luz los primeros riesgos, la sociedad ya considera, paradójicamente, que limitar las redes supondría una intolerable limitación de derechos.

Ningún Estado, por ejemplo, quiere quedar al margen del comercio electrónico, pero esto no garantiza que el riesgo sea soportable en términos jurídicos. Si P. Bonfante[30] o S. Perozzi[31] representaban al Estado y a la familia en los mismos términos, pero a diferente escala, quizás sea la hora de entender que la realidad virtual está hecha a escala de la vida real (física), y que nunca concebiríamos la vida social real sin límites o respeto al derecho, o libertad, ajeno. Esta necesidad de la red, esta desinformación y este uso y abuso de lo tecnológico es, lógicamente, aprovechada por los nuevos ciberdelincuentes, porque es en la red donde están hoy en día los datos, la intimidad, el valor económico, los intereses, etc. De ahí que se sostenga que la inteligencia artificial juega un papel nuclear en el devenir cotidiano de la ciudadanía con las consiguientes implicaciones jurídicas, entre otras muchas (D.L. Morillas Fernández[32]).

Que la ciberactividad es un fenómeno de especial trascendencia e importancia lo evidencia la propia ONU cuando, en año 2015, afirmó que uno de los principales elementos impulsores de la ciberdelincuencia contemporánea y del uso creciente de pruebas digitales es el desarrollo de la conectividad electrónica global. Hoy existen casi 3.000 millones de usuarios de Internet, cerca del 40% de la población mundial[33]. No debe extrañar, por ello, que se haya mantenido, a nivel jurisprudencial, que lamentablemente la ciberdelincuencia sigue su auge exponencial[34]. Como resalta J.M. Palma Herrera[35], la sociedad del siglo XXI es la sociedad del ocio y del consumo, pero es también cada vez más, una sociedad que se siente amenazada por la aparición de nuevas fuentes de peligro asociadas,

[30] P. Bonfante, *Corso di diritto romano*, Giuffré, Milano, 1963.

[31] S. Perozzi, *Istituzioni di Diritto Romano*, F. Vallardi, Milano, 1947, pp. 311 y ss.

[32] D.L. Morillas Fernández. *Implicaciones de la inteligencia artificial en el ámbito del Derecho Penal*, en esta obra.

[33] ONU. (A/CONF.222/12) *13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional*, celebrado el 2 de febrero de 2015, p. 7.

[34] SAP Barcelona de 9 de julio de 2020 (ECLI:ES:APB:2020:7301), p. 3.

[35] J.M. Palma Herrera, *Inteligencia artificial y neurociencia. Algunas reflexiones sobre las aportaciones que pueden hacer al Derecho Penal*, en esta obra.

paradójicamente, a ese progreso y bienestar.

La ciberseguridad se está configurando como un derecho de los ciudadanos y un deber de los Estados de garantizar el libre ejercicio de los derechos fundamentales y libertades públicas en la red, promoviendo medios para la seguridad e integridad de las infraestructuras y la información. En el caso de los robots inteligentes existe una interconexión continua e instantánea entre el mundo físico y digital y se deberá velar simultáneamente por la seguridad en ambos entornos. Los robots inteligentes, como sistemas físicos cibernéticos, no están exentos de sufrir ataques y las principales amenazas a las que se enfrentan son el malware, el ciber espionaje, denegaciones de servicio, pérdida de información, spam, phishing o daño físico entre otros (I. Lledó Benito[36]).

3. *Límites normativos*

Lo que no está tan claro es qué institución (política) puede poner barreras normativas a la ciberactividad, máxime cuando estos límites son percibidos como restricción de falsos derechos por el electorado del que dependen. Un electorado que, a su vez, y para evidenciar una circularidad en bucle, será manipulado con opiniones, a favor y en contra, que serán generadas a través de esas mismas redes sociales que pretenden ser reguladas. Un ejemplo lo vemos a diario en Twitter; o en las cámaras de seguridad ciudadana: Todos queremos la seguridad que nos brindan, al tiempo que nos consideramos espiados. Es preciso llegar a ese punto de equilibro aristotélico como medida de la virtud: cualquier solución implica, paradójicamente, una restricción, un nuevo problema.

Han sido varios los intentos de regular aspectos concretos de la ciberdelincuencia, sobre todo de aquella parte que afecta a la seguridad y protección de los datos que es, al fin y al cabo, el origen de toda actividad ciberdelictiva. Como en su día señalamos (J. Pérez-Arias[37]), las siguientes normas internacionales resultan de interés:

1.- Como primera norma supranacional, dentro del ámbito territorial europeo, debemos partir de la ya clásica Directiva 95/46/CE, de 24 de

[36] I. Lledó Benito, *Ciberseguridad Versus Ciberdelincuencia*, en *El derecho penal, robots, IA y cibercriminalidad: desafíos éticos y jurídicos. ¿Hacia una distopía?*, Dykinson, Madrid, 2022, p. 18.

[37] Pérez-Arias, *Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal*, cit., p. 178-179.

octubre de 1995; norma que, actualmente, se encuentra derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Esta norma inició la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Se trata de una norma que, dentro del ámbito que estudiamos, es secundaria e indirecta, ya que su objeto no es, como resulta evidente (dado el año de su aprobación), la realidad cibernética y, sobre todo, el contexto de protección de datos que circulan en la red, tal y como lo conocemos hoy en día[38].

Sin embargo, en esta Directiva 95/46/CE se procuró tutelar los datos personales almacenados en bases de datos de numerosos organismos públicos y privados, cuya nueva trascendencia permite su aplicación para un sinnúmero de fines diversos, que van desde la seguridad pública y la defensa del Estado (v.gr. registros de naturaleza penal) hasta la ponderación de riesgos en la concesión de préstamos o servicios (G. Eduardo Aboso[39]).

2.- El llamado Convenio de Budapest (Convenio sobre la ciberdelincuencia) de 23 de noviembre de 2001, cuyo objetivo, tal y como expone su preámbulo, es satisfacer la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional. Y todo ello a partir de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de redes informáticas. En definitiva, el Convenio sobre Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001, supone la respuesta a la necesidad de tener medios eficaces de cooperación para la lucha contra la cibercriminalidad (M.C Rayón Ballesteros/J.A. Gómez Hernández[40])

Es de destacar la capacidad de antelación que tuvo este convenio, que ya en el año 2001, cuando las redes aún se encontraban en un momento muy incipiente (respecto, al menos, de consumidores particulares y finales), se percató del peligro de las redes informáticas y la información

[38] Puede profundizarse más en A. Palma Ortigosa, *Decisiones automatizadas y protección de datos*, Dykinson, Madrid, 2022.

[39] G. Eduardo Aboso, *Derecho Penal Cibernético. La cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación*, B de f, Buenos Aires, 2017, p. 59.

[40] M.C. Rayón Ballesteros, J.A. Gómez Hernández, *Cibercrimen: particularidades en su investigación y enjuiciamiento*, en «Anuario jurídico y económico», Número 47, enero 2014, p. 212.

electrónica cuando éstas fueran utilizadas igualmente para cometer delitos y del riesgo de que las pruebas relativas a dichos delitos fueran almacenadas y transmitidas por las redes (así se expresa el preámbulo del convenio). En aquel año ya se hablaba de la necesidad de que los Estados firmantes (España lo ratificó, no obstante, en el año 2010[41]) incorporaran en la regulación sustantiva penales determinados delitos que, poco a poco, y en años posteriores, fueron quedando integrados en el código penal español, a partir de sus diversas reformas[42]. Estas figuras eran los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (artículos 3 a 6 del convenio); delitos informáticos, propiamente dichos (artículos 7 a 8); delitos relacionados con el contenido (en materia de pornografía infantil, art. 9); delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10), así como otras disposiciones en materia de Derecho Penal general.

3.- La Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. La etiología de la norma la plasma su misma exposición de motivos, al indicar que se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea.

4.- Lo sorprendente es que el legislador español, en el intento de estar a la 'vanguardia', transpone esa decisión marco en el mismo año que Europa había propuesto una Directiva[21] para derogarla. No es de extrañar, puesto que la decisión marco era de 2005 y la reforma del código penal

[41] Véase Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE núm. 226, de 17 de septiembre de 2010). Dicho Convenio entró en vigor para España el 1 de octubre de 2010, de conformidad con lo establecido en su artículo 36.4.

[42] Como afirma N.J. De la Mata Barranco, las transposiciones europeas se vienen haciendo en nuestro Código Penal desde el respeto a la sistemática tradicional del mismo, en su caso con el habitual recurso a los títulos, capítulos o artículos bis, ter, etc. (N.J. De la Mata Barranco, *Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 97 CP). El concepto de de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación*, en «Cuadernos de política criminal», segunda época, Núm. 118, mayo 2016, p. 55.

tuvo lugar cinco años después. Afortunadamente para el legislador español, esta Directiva no fue aprobada hasta el año 2013, mediante Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI. No será, pues, hasta la reforma del código penal del 2015 cuando el legislador español traspusiera la Directiva 2013/40/UE[22]. La misión de esta reforma fue la de pretender superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea (preámbulo, punto XIII, LO 1/2015).

El trasfondo de toda esta normativa internacional trata de conocer la seguridad de los sistemas de información en sí mismos considerados y, en su caso, la confidencialidad de los datos (y su integridad y disponibilidad frente a conductas de daños) que, por una parte, permiten el correcto funcionamiento de tales sistemas y, por otra, garantizan el funcionamiento de una sociedad cada vez más vinculada a dichos sistemas (N.J. De la Mata[43]). Que la cuestión no es sencilla lo demuestra que, a día de hoy, no exista en el derecho penal español un delito informático en sentido estricto y tampoco un concepto penal de cibercriminalidad o ciberdelito, y ese es el punto preocupante del que partimos. En efecto, el Código Penal español, a fuerza de tratado internacional, ha ido introduciendo, poco a poco, delito a delito (allá donde fuera necesario) determinadas modalidades delictivas, que incluían lo informático como medio comisivo autónomo y específico, pero en ningún caso ha denominado a alguno de ellos delito informático, ni mucho menos ha creado un título autónomo a este fenómeno criminal (J. Pérez-Arias[44]). La falta de una regulación específica evidencia la complejidad del tratamiento jurídico de este fenómeno criminal. Como señala I. Benítez Ortuzar[45], ni existe ni es fácil que se consensue un concepto unitario perfectamente definido de 'delito informático' que incluya todas las modalidades delictivas que tienen en los datos incorporados en los sistemas informáticos o en los propios

[43] Mata Barranco. *Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 97 CP). El concepto de de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación*, cit., p. 57.

[44] Pérez-Arias, *Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal*, cit., p. 176.

[45] I. Benítez Ortúzar, *Ciberdelitos: la implementación en el ordenamiento interno de los acuerdos internacionales en materia de ciberdelincuencia*, en *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0* (Coord. M.J. Cruz Blanca, I. Lledó Benito), Dykinson, Madrid, 2021, p. 81.

sistemas informáticos el objeto o el instrumento del delito.

Con todo, y como se ha señalado por la jurisprudencia[46], los ciberdelitos -aquellos que ya tienen respaldo normativo- deberían establecer también penas específicas (como la inhabilitación especial) y, sin embargo, ninguna se establece específicamente relacionada con las TIC. De hecho, si prestamos atención a las figuras delictivas más próximas a la cibercriminalidad, observamos que las penas previstas son las tradicionales penas de prisión y multa. En definitiva, hay todavía mucha distancia que recorrer, porque son muchas las carencias e imprecisiones existentes en la normal penal.

4. *Problemas procesales ¿*vs*? problemas penales*

El debate debe girar en torno a dos rasgos que se han de conciliar, y que resulta difícil que lo hagan: Riesgo y resultado. En ambos casos, nos enfrentamos con inconvenientes de índole procesal y penal. Respecto de los problemas procesales, nos encontramos con dos factores esenciales a tener en cuenta: la desterritorialización y el anonimato. Problemas éstos que, a la postre, también generarán disfunciones en el derecho penal sustantivo, como es el derecho aplicable[47] o la identificación última del

[46] Entre otras, puede verse la SAP Barcelona, de 6 de mayo de 2015 (ECLI: ES:APB:2015:2946), p. 5. Como sigue indicando esta Sentencia, el objetivo de la imposición de prohibiciones de uso de las TIC en los EE.UU. no es apoyar la rehabilitación, ni tan solo incapacitar completamente y constantemente al sujeto, sino limitar simplemente las oportunidades delictivas y, sobre todo, introducir una infracción técnica susceptible de ser detectada a medio plazo y que justifique la revocación de la medida y el retorno a la prisión. Por lo contrario, la situación en nuestro país es la opuesta. Como se ha visto, nuestro marco legal continúa orientado hacia un modelo rehabilitador, en el cual las medidas de control cumplen sobre todo una función auxiliar del tratamiento y casi no están reguladas, de manera que sería muy cuestionable un sistema de control del de las condiciones tan agresivo como el norteamericano. Por otra parte, a pesar de algunas mejoras en los últimos años, en la práctica nuestro aparato de ejecución penal en el entorno comunitario es muy débil, a duras penas puede hacer frente a las necesidades más urgentes y no está en condiciones de llevar a cabo un control intensivo.

[47] En igual sentido, cuando afirma que a efectos procesales, hay que matizar que la conducta delictiva puede tener su origen en uno o varios países y los resultados producirse en otro u otros, incluso puede resultar difícil determinar dónde se ha cometido la acción o por parte de quién. Obviamente esto afecta a la competencia jurisdiccional, a la ley penal aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento, ya que la regla general tradicional se refiere al lugar de comisión del delito o locus comissi delicti (principio de territorialidad) contenido en la Ley Orgánica del Poder

autor. La ciberdelincuencia, pues, representa una amenaza global, técnica, transfronteriza y anónima, y comprensiva de cualquier tipo de actividad ilegal (G. Martínez Atienza[48]).

Si se quiere llegar a una categorización del cibercrimen es importante asimilar las características que posee ese nuevo fenómeno (J. Pérez-Arias[49]). Entre todas las características que podrían desarrollarse sobre las tecnologías de la información y la comunicación (TIC), nos concentraremos en tres: 1. la inmediatez de las comunicaciones a distancia, 2. la posibilidad de la realización de acciones masivas (automatizadas o no) y 3. la posibilidad de realizar acciones con un determinado nivel de anonimato (M. Temperini[50]).

En cuanto a la desterritorialización, la red cuenta con un importante rasgo característico: se trata de un espacio sin fronteras. Es la verdadera globalización. Esto hace que muchos de los ataques sean cometidos desde servidores o ubicaciones extranjeras, que impiden, por propia jurisdicción, avanzar (de un modo fructífero) en una investigación policial y/o judicial. Se nos podrá indicar, con acierto, que una correcta interpretación del artículo 23 de la Ley Orgánica del Poder Judicial permitiría investigar un hecho delictivo con estos caracteres transfronterizos. Sin embargo, a nivel práctico (no teórico ni hermenéutico), esa investigación no fructificaría en un resultado apto para su enjuiciamiento. Pensemos que un país extranjero (sobre todo extracomunitario) no facilitará, en muchos casos, datos o identidades de sus propios nacionales, sobre todo cuando estemos hablando de ciertos países, que se han convertido en un auténtico territorio offshore (por referencia analógica al paraíso fiscal) de la ciberdelincuencia. Todos tenemos, al menos, uno o dos países en mente.

Incluso delinquiendo desde España, la ingeniería informática y el sistema de redes permite simular una ubicación falsa gracias al empleo de un proxy encadenado o una VPN. Por tanto, los jueces españoles van a encontrar serios inconvenientes en su labor judicial, cuando una investigación se tiene que realizar, en su totalidad (no en algún aspecto concreto, que sí es frecuente) con diligencias para las que se necesitan el completo auxilio y/o cooperación de terceros países. Y, aun cuando eso se produzca, luego

Judicial. (Rayón Ballesteros, Gómez Hernández, *Cibercrimen: particularidades en su investigación y enjuiciamiento*, cit., p. 216).

[48] G. Martínez Atienza, *El blanqueo de capitales y su sanción administrativa y penal*. «Revista de Derecho vLex», número 202, Marzo 2021, p. 1.

[49] *Ibídem*, p. 191.

[50] M. Temperini. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*, en *Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet*, Erreius, Buenos Aires, 2018, p. 52.

sería complicado abrir juicio oral, porque se requiere presencialidad de los acusados. En la actualidad resulta poco frecuente encontrar jurisprudencia que analice la cuestión de la inteligencia artificial en el sentido que aquí analizamos (más allá de tratarla como medio comisivo específico en algunas figuras delictivas), y eso es la prueba evidente de que resulta complicado que un asunto de esta naturaleza llegue a los tribunales. De ahí que, en palabras de D.L. Morillas Fernández[51], la descripción de la inteligencia artificial en la jurisprudencia penal española no cuente con una excesiva representatividad si nos atenemos a su descripción taxativa.

El anonimato es el otro gran inconveniente que, desde perspectivas procesales (luego veremos que también de derecho penal sustantivo), nos debe llamar la atención. En efecto, en la red sólo existe un sistema de identificación: la dirección IP (Internet Protocol). Como se tiene afirmado, cuando un terminal se conecta a Internet es necesario que disponga de un número que lo identifique de forma unívoca, que lo diferencie de cualquier otro ordenador en la red y permita localizarlo, de igual forma que las direcciones postales distinguen cada calle y cada casa de cualquier otra en el mundo. Cuando un usuario solicita o envía una información, se genera una carta o paquete en el que se escribe tanto la dirección destino como el remitente (L. Salvador Carrasco[52]).

Pero imaginemos este protocolo a nivel o escala mundial y con toda la tecnología disponible, y cuyos servicios de anonimización permitirán convertir en papel mojado todos los protocolos de identificación. De ahí que se señale que uno de los mayores escollos en materia de responsabilidad penal en el ámbito de la comisión de los llamados ciberdelitos se vincula con el papel que cumplen las empresas proveedoras de servicio en Internet por los delitos cometidos por terceros (G. Eduargo Aboso[53]). La anonimización, junto a la desterritorialización, son los auténticos obstáculos procesales de difícil superación, ya que no puede haber proceso sin tribunal con jurisdicción (territorial, como presupuesto del proceso[54]) ni sin persona a quien investigar, imputar y finalmente acusar.

Por lo que hace al derecho penal, el principal problema lo tenemos en

[51] Morillas Fernández, *Implicaciones de la inteligencia artificial en el ámbito del Derecho Penal*, en esta obra. p. 23.

[52] L. Salvador Carrasco, *Redes de anonimización en internet: cómo funcionan y cuáles son sus límites*, en «Revista de Instituto Español de Estudios Estratégicos», número 16/12. 2012, p. 3.

[53] Eduardo Aboso. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación*, cit., p. 425.

[54] V. Gimeno Sendra, *Derecho penal procesal*, Civitas-Thomson Reuters, Navarra, 2012, pp. 160-161.

la difícil -si no imposible[55]- conexión causal entre la conducta del autor y el algoritmo en el que finalmente se desencadena la conducta ideada. El problema penal es peliagudo, porque todo se hace partir de un algoritmo que aprende en la red, y que no solo depende del autor intelectual (persona física), sino del desarrollo autónomo que aquella programación generará una vez entre en la red. Es la llamada inteligencia artificial (y que tanta utilidad ofrece cuando es Alexa, Siri o nuestro teléfono quien la tiene). Estamos, como se ha dicho, ante una misma tecnología que facilita la comunicación pero que puede explotarse con fines terroristas y delincuenciales (S. Morán Blanco[56]). Al ser difícil conectar causalmente el resultado con la conducta de un sujeto (porque intervienen muchas concausas), será fácil imaginar que también resultará poco fácil individualizar al sujeto primario que hay detrás de esa inteligencia artificial. De ahí la importancia de delimitar y enfocar correctamente el problema informático en su relación con el derecho penal[57].

Posiblemente, sea más necesario formular preguntas que improvisar respuestas. Preguntas, cuyas respuestas futuras, pueden generar algo de luz a este fenómeno criminal. Desde el punto de vista penal, ¿estamos tan solo ante un mero medio comisivo más (delito informático) o ante una realidad nueva, con tratamiento jurídico diferenciado (sujetos (v.g. *bots*), bienes jurídicos afectados (v.g. seguridad ciberespacial), conductas, víctimas, finalidades etc.)? Es evidente que aquí hay dos tendencias claramente: Aquella que podríamos tildar de regla general, que considera que el fenómeno informático no es más que un medio comisivo, y que los delitos afectados siguen siendo los tradicionales, sin que el medio comisivo cambie o afecte el tratamiento penal tradicional de la figura; y de otro lado, una nueva tendencia que considera que estamos ante una nueva realidad, esto es, ante nuevos delitos, no tratados específicamente (aunque pudieran encajar de manera alambicada en alguna modalidad concreta) en el código penal. Es el caso, por ejemplo, del secuestro de datos (*ransomware*) o del falso antivirus (*Scareware*). Decidir si estamos ante una tendencia u otra, haría variar no solo el estudio y la sistemática del fenómeno, sino también la técnica del legislador (J. Perez Arias[58]).

Cuanto más queramos abstraer el fenómeno cibernético, mayor

[55] Así lo será en numerosos casos.

[56] Morán Blanco, *La ciberseguridad y el uso de las tecnologías de la información y la comunicación (tic) por el terrorismo*, cit., p. 197.

[57] Muy en la línea de como se hizo, en su día, con el delito de tráfico de drogas.

[58] Pérez-Arias, *Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal*, cit., p. 192.

problema habrá para legislar sobre ello. Si, en cambio, lo informático (aparte su naturaleza compleja) se considera, a estos efectos, un mero medio comisivo[59], obviamente su tratamiento jurídico no pasará de ser un añadido descriptivo al tipo que proceda. Este es el modo en el que, hoy en día, se regulan los delitos relacionados con el ciberespacio en el código penal español.

Pero es que, además, al derecho penal no le puede resultar indiferente el anonimato al que antes hacíamos referencia. En efecto, desde perspectivas penales, no hay posibilidad de delito ni de consecuencias penales sin sujeto. Y es evidente que, en multitud de casos, el anonimato no va a permitir imputar objetivamente la conducta a persona determinada ni determinable. No estamos hablando de la culpabilidad o no del sujeto, sino de algo previo, de la existencia o no de sujeto a quien atribuir un resultado que se presenta como delictivo. Sin lugar a dudas, desde perspectivas prácticas, es el proceso quien debe individualizar el sujeto responsable; pero desde una visión técnica penal y técnica legislativa, se debe analizar si la conducta dañosa es el producto o resultado de una persona o de un conjunto algorítmico que aprende de manera autónoma en el ciberespacio, y que ya no es controlado por ningún sujeto. Sobre esto profundizamos en el siguiente apartado.

5. *Sujeto activo, resultado y culpabilidad: juicio de probabilidad estadística*

La consecuencia de este aprendizaje autónomo (característico de la inteligencia artificial) es que el resultado final (aquel que culmina con la lesión concreta del bien jurídico) puede no haber sido, ni siquiera, imaginado con precisión por el autor, más que a título de juicio remoto de probabilidad. Por tanto, el autor quiere, pero solo puede esperar, lo que nos lleva a una forma de culpabilidad dolosa híbrida o de tipo mixto, y con esto, a otro problema: La contingente voluntad[60] haría inexplicable el uso

[59] La problemática de si lo informático es un medio comisivo o si supone un nuevo tipo de delito también se lo plantean S. Garat, J. Reale, *La reforma penal en materia de cibercrimen en la República Argentina*. en *Cibercrimen II* (Dir. D. Dupuy), B de f, Buenos Aires, 2018, p. 506.

[60] Voluntad entendida como finalidad perseguida y buscada de propósito. Es contingente, porque puede estar presente, o puede no estarlo, por lo que siempre quedará el margen de duda de hasta qué punto el comportamiento del sujeto puede imputarse a título de dolo, aunque sea dolo eventual.

directo del delito doloso, si se contempla, incluso como mera hipótesis, el resultado como fruto del puro accidente. En efecto, en la mayoría de las ocasiones, la forma de culpabilidad característica del autor (desde una perspectiva empírica y no teórica) será la del dolo eventual, lo que, si bien permite hablar de la consciencia de la acción, anticipa la fina línea que separa la mera culpa o imprudencia consciente de aquel tipo de dolo.

El problema no es nada novedoso en el derecho penal, aunque es cierto que hoy se incluye un nuevo elemento a la discusión: No se trata solo de estar ante un sujeto que se representa el resultado como posible o probable, sino ante un sujeto que, aunque quisiera tener certeza de que el resultado se va a producir, no tiene capacidad de valorar conscientemente si quiera su causación probable. Es obvio que nos referimos a la ciberdelincuencia más profunda (la que de verdad es preocupante), aquella que no consiste en un mero ataque de terminal a terminal de fácil averiguación causal. No debe olvidarse que, en todos estos casos, la conducta desplegada se produce mediante lenguaje binario sobre datos anónimos al azar, no mediante conductas humanas sobre sujetos conocidos. Es el llamado *aprendizaje no supervisado* con *capacidad de autoorganización* (J.G Corvalán[61]).

No se trata de imputar el resultado a bulto, sino de hacerlo con absoluto respeto a una causalidad adecuada y relevante, que no solo debe existir, sino ser la prueba de la existencia de una conducta clara, causalmente directa y determinante del resultado. Pese a esto, se mantiene que los algoritmos trabajan de forma superficial (no pueden abstraer o valorar en conjunto) y sin basarse en relaciones causales (solo en correlaciones significativas)[62]. No obstante, si la causalidad no es posible definirla con exactitud, o el resultado es obra de la previsibilidad tan solo, no es posible hablar de conducta dolosa en sentido estricto; y solo en el segundo caso sería posible imputarla a título imprudente o, en el mejor de los casos, como dolo eventual, dependiendo del grado de probabilidad con la que se representó el resultado el autor (con lo que ello supone, además, cuando se ha de decidir imputar un delito doloso, en el que el margen de exactitud de ese juicio de probabilidad se representa impreciso siempre). Si atendemos al resultado, en definitiva, se tendría que castigar la conducta como imprudente (de existir en esa figura concreta, ex artículo 12 del código penal español), aun cuando el origen de

[61] J.G. Corvalán. *Presentación: Inteligencia artificial. Automatización y predicciones en el Derecho*, en *Cibercrimen III* (Dir. D. Dupuy, J.G. Corvalán), B de f, Buenos Aires, 2020, p. 31.

[62] C. Souza de Menezes, J.R. Agustina. B*ig Data, inteligencia artificial y policía predictiva*, en *Cibercrimen III* (Dir. D. Dupuy/J.G. Corvalán), B de f, Buenos Aires, 2020, p. 160.

la acción sea claramente doloso. Imputar un delito doloso, en estos casos, sería una clara interpretación contra reo. Y ello, como decíamos arriba, en el supuesto remoto de que ese resultado concreto pudiéramos imputarlo a un sujeto concreto, que no será muy frecuente.

Y esto es una nueva disfunción sustantiva, pues nadie duda del carácter doloso de la conducta, pero la garantía del derecho penal no debe ceder a la utilidad social que reporta el castigo; castigo que, de producirse en estas condiciones, iría más allá de la culpabilidad[63], lo que se encuentra no solo en contra de la norma constitucional[64] sino de los artículos 5[65] y 10[66] del código penal español. Dicho de otro modo, aun pudiendo demostrar y valorar el resultado (con su correspondiente lesión del bien jurídico), como consecuencia causal de la conducta primaria del sujeto, quedaría por definir a título de qué forma de culpabilidad puede serle reprochado el delito. Y no es que se mezclen categorías dogmáticas (la causalidad es propia del tipo de injusto y el dolo[67] y la imprudencia de la culpabilidad); pero es evidente que cuando todo se difumina (y así ocurre con esta forma de criminalidad anónima), al final todo se mezcla y confunde. Sin hecho criminal imputable objetivamente (lesión del bien jurídico o fin de protección de la norma, incremento del riesgo, y causalidad), difícilmente podremos imputar subjetivamente el resultado a una persona concreta.

En otro caso, se produciría una identificación entre bien jurídico y objeto de la conducta, que conduciría al renacimiento del versari in re illicita[68] (y a la consiguiente abolición, si quiera parcial, del principio de

[63] La culpabilidad es el fundamento y el límite de la pena, tal y como recuerda M.I. González Tapia. *Neurociencias e imputabilidad: recapitulando*, en esta obra.

[64] Como mantuvo la STC 150/1991, «La CE consagra sin duda el principio de culpabilidad como principio estructural básico del Derecho Penal» (STS 150/1991, de 4 de julio de 1991, ECLI**:** ES:TC:1991:150)

[65] Artículo 5 del código penal español: No hay pena sin dolo o imprudencia.

[66] Artículo 10 del código penal español: Son delitos las acciones y omisiones dolosas o imprudentes penadas por la Ley.

[67] Salvo en aquellos delitos con elemento subjetivo, en cuyo caso el dolo podría estar presente desde el mismo análisis de la conducta.

[68] En cuanto al Versari in re illicita la entendemos en el sentido explicado por M. Cobo del Rosal, esto es, en su forma tradicional, y más rigurosa, el versari implica la imputación a título de dolo consecuencias fortuitas o respecto de las que solamente existe culpa; Sin embargo, con el transcurso del tiempo, han prevalecido formas atenuadas, en las cuales únicamente se responde a título de dolo por las consecuencias no queridas cuando concurre, al menos culpa respecto de ellas o bien se imputan las consecuencias fortuitas, pero no a título de dolo, sino al más leve de imprudencia (M. Cobo del Rosal, T. Vives Antón, *Derecho Penal. Parte General*, Tirant lo Blanch, Valencia, 1991, p. 489).

legalidad y del principio de culpabilidad), determinándose el delito por la causación del resultado y la culpabilidad por la coincidencia gramatical entre este resultado (que coincidiría con la conducta) y el tipo descrito en la norma (J. Pérez-Arias[69]).

En efecto, la conducta, a veces, no funciona o no consigue el objetivo donde el autor esperaba, aunque se haya puesto el mecanismo en marcha, lo que nos lleva a la dificultad de vincular a una persona determinada con un hecho concreto y un resultado esperado. En palabras de Jakobs, el comportamiento de un autor o participe se define como causa determinante del curso lesivo [70]. Por ello, al margen de figuras concretas allá donde sea posible (una estafa, injurias graves, pero no a través de bots, que nos llevaría a la misma problemática) la solución no pasaría, en todos los casos, por tipificar la cibercriminalidad como derecho penal del resultado, sino como derecho penal de peligro (o de riesgo), lo que ello ya de por sí comporta.

De ahí, que el legislador, si quiere ofrecer una respuesta jurídico penal eficaz, deba tipificar conductas de peligro hipotético o potencial, donde el objeto de investigación e imputación no sea el resultado, sino la idoneidad de la conducta cibernética para originar un riesgo grave en el bien jurídico protegido (adelantando con ello la barrera de protección, y sin exigir llegar a un resultado de imposible imputación causal, que comportaría la plena desprotección del bien jurídico). Se trataría de un delito de actividad, cuyo merecimiento de pena, en palabras de H. Jescheck/T. Weigend[71], descansa sobre la peligrosidad general de la acción típica para determinados bienes jurídicos.

Por tanto, hay mucho de probabilidad e intención, y muy poco -a veces nada- de conexión directa (objetiva y subjetiva) con un resultado concreto (en términos naturalísticos). Mas aún, en la mayoría de los casos, la conducta final lesiva y el resultado ni siquiera serán conocidos, ni esperados, ni imaginados, con carácter previo por el autor. La peligrosidad del ciberdelincuente estriba en que este lanza un producto (que busca solo y crece solo), y solo tiene que esperar el resultado (si lo hay). Es, en realidad, una caza con red (J. Pérez-Arias[72]).

[69] Pérez-Arias, *Sistema de atribución de responsabilidad penal a las personas jurídicas*, Dykinson, Madrid, 2014, pp. 161-162.

[70] G. Jakobs. *Concurrencia de riesgos: curso lesivo y curso hipotético en el Derecho penal*, en «El Derecho Penal. Lecciones y Ensayos», Nº 54, 1990, p. 54.

[71] H. Jescheck, T. Weigend, *Tratado de Derecho Penal. Parte General* (trad. M. Olmedo Cardenete). Comares, Granada, 2002, p. 283.

[72] Pérez-Arias, *Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal*, cit., p. 189.

Esto nos llevará, por otro lado, a la impunidad -por cuestiones procesales- de muchas de las conductas que actualmente abundan, pero sería desproporcionado teorizar al contrario y a contracorriente, esto es, castigando, a través de delitos de resultado, conductas que, en términos causales, no están determinadas con plena precisión y seguridad (lo que ello comporta para la antijuridicidad de la acción y para la culpabilidad del sujeto). En efecto, no sería posible, desde una perspectiva jurídico penal y constitucional, atribuir a un sujeto la comisión de un hecho, cuando no existe prueba real que desvirtúe correctamente la presunción de inocencia sobre su autoría.

Esto resulta pacífico cuando se trata de otra tipología delictiva, y no hay motivo para no aplicar el mismo principio a la cibercriminalidad: Si no existe prueba, el tribunal no puede, en ningún caso, desvirtuar la presunción de inocencia mediante hipótesis contra reo o argumentos alambicados y especulativos. De hecho, y como se ha señalado en reiterada jurisprudencia, es ya una doctrina consolidada que la presunción de inocencia debe entenderse como un derecho a no ser condenado sin pruebas de cargo válidas. Ello implica que en la Sentencia condenatoria deben expresarse las pruebas de cargo que sustentan la declaración de responsabilidad jurídico-penal, las cuales, a su vez, han de proceder de verdaderos actos de prueba obtenidos con todas las garantías que exigen la Ley y la Constitución, y normalmente practicados en el acto del juicio oral (STC 171/2000[73], 26

[73] ECLI:ES:TC:2000:171, p. 5. Esta interesante sentencia del Tribunal Constitucional español sigue diciendo que este Tribunal ha admitido asimismo que la prueba de cargo puede ser por indicios, cuando el hecho objeto de prueba no es el constitutivo de delito sino otro intermedio que permite llegar a él por inferencia lógica, siempre que se cumplan los siguientes requisitos: a) la prueba indiciaria ha de partir de hechos plenamente probados; y b) los hechos constitutivos de delito han de deducirse de esos hechos completamente probados a través de un proceso mental, razonado y acorde con las reglas del criterio humano, explicitado en la Sentencia. La falta de concordancia con las reglas del criterio humano o, en otros términos, la irrazonabilidad, se puede producir, tanto por falta de lógica o de coherencia en la inferencia, cuando los indicios constatados excluyan el hecho que de ellos se hace derivar o no conduzcan naturalmente a él, cuanto por el carácter excesivamente abierto, débil o indeterminado de la inferencia. El control de dichos requisitos debe ser extremadamente cauteloso, al carecer este Tribunal de la necesaria inmediación de la actividad probatoria, que sólo tiene lugar en presencia del órgano judicial que ha de decidir el proceso y con intervención de las partes. No obstante lo anterior, las especiales características de la prueba indiciaria y la elaboración subjetiva de su valoración por el Juez o Tribunal que haya presenciado la prueba hacen que el Tribunal Constitucional deba exigir en las resoluciones judiciales que se someten a su conocimiento por esta causa una motivación suficiente de la inferencia y del resultado de la valoración, de tal manera que una y otro, en este ámbito de enjuiciamiento, 'no resulten tan abiertos que quepan tal pluralidad de conclusiones alternativas que ninguna de ellas pueda darse por probada'.

de Junio de 2000).

En estos casos, la conducta no podría ser objeto de imputación objetiva, ya que, a pesar de poder valorar, en el mejor de los casos, el incremento del riesgo con la conducta primaria del agente (aquella que pone en circulación el algoritmo, tras su programación) y la probable y/o previsible lesión del bien jurídico (fin de protección de la norma), no existiría técnicamente, salvo que aceptemos la divagación argumental, la debida e individualizable relación causal entre el hecho primario del agente y el hecho final concreto (no aquel primario) y el resultado lesivo que se termina produciendo.

Ni siquiera podríamos hablar de la llamada causalidad cumulativa, aunque estemos ante varios actos que terminan produciendo -todos ellos juntos- el resultado. Y no lo estamos, porque el aprendizaje del algoritmo autónomo no es, técnicamente, un acto consciente (sobre la causalidad) de la persona natural (del programador), por lo que difícilmente puede considerarse ese acto algorítmico de aprendizaje como una conducta consciente y subsiguiente de la persona. Además de ello, el acto algorítmico de aprendizaje no es por sí solo capaz de producir el resultado sin ese acto primario, ni del acto primario podemos derivar como consecuencia causal directa y necesaria la producción del resultado, sin tener en cuenta aquellos otros sucesos algorítmicos posibles y autónomos posteriores. En palabras de S. Mir Puig[74], existiría causalidad cumulativa cuando el resultado fuera causado por dos o más condiciones cada una de las cuales resultó suficiente por sí sola para producirlo. Y, en todo caso, tendríamos que estar ante actos humanos en sentido estricto, esto es, ante manifestaciones conscientes de la voluntad de la persona, cualidad inexistente, por definición, en un acto algorítmico artificial autónomo.

Por tanto, en nuestra opinión, la mayoría de las conductas derivadas de inteligencia artificial escaparían de los parámetros de previsibilidad racional, y entrarían por completo en el terreno de la predicción estadística, hecho este absolutamente distinto. Si por previsibilidad se ha de entender la posibilidad de prever la conducta de otros sujetos (I. Lifante Vidal[75]), la predicción estadística requiere método científico, porque el resultado no es previsible, sin más, sin llevar a cabo un tratamiento y estudio sobre la combinación matemática de datos que explique la causalidad (con su margen de error correspondiente). Por tanto, la conducta escapa de la previsibilidad tradicional, ya que la causación se convierte en una

[74] S. Mir Puig. *Derecho Penal. Parte General*, Reppertor, Barcelona, 2012, p. 250.

[75] I. Lifante Vidal. *La relevancia de la previsibilidad jurídica*, en *DOXA. Cuadernos de Filosofía del Derecho. Edición especial*, Marcial Pons, Madrid, 2017, p. 145.

predicción de difícil intuición a priori. De ahí que consideremos el delito de peligro como única forma no solo de anticipación de la lesión impredecible y dudosa (en términos causales), sino para poder valorar como intencionada una conducta claramente peligrosa y dolosa. En otro caso, se produciría la paradoja de necesitar inteligencia artificial -no parámetros jurídicos- para poder medir, a su vez, la responsabilidad penal de un sujeto que actúa -hecho relevante- a través de una fórmula algorítmica que auto-aprende (hecho no sujeto a control humano). Quizás no tarde mucho en implantarse esto que se ha dado en llamar el '*juez-robot*[76]'. No debemos olvidar que la ciencia forense es una de las grandes beneficiarias de estas nuevas tecnologías. Sería, como señala J. Peris Riera[77], algo muy parecido a lo que ocurrió, en su día, con las huellas dactilares o el ADN, avances ambos sin los cuales difícilmente podríamos explicar hoy los resultados que se producen en la averiguación del delito y persecución del culpable.

Quedaría por valorar si la mera activación del algoritmo permitiría en un momento posterior concretar el peligro para el bien jurídico pues, en ese caso, el delito debería ser de peligro concreto[78] (convirtiéndose el riesgo concreto en auténtico elemento del tipo). En otro caso, esto es, impedir que cada intérprete pueda analizar el peligro de una manera diferente (sobre todo partiendo de que estamos ante un peligro estadístico, que permitiría múltiples interpretaciones, a favor y en contra) nos llevaría a configurar la conducta como delito de peligro abstracto (de mera actividad), haciendo innecesaria, con ello, la prueba sobre el efectivo riesgo hacia el bien jurídico. No obstante, se ha de matizar que el delito de peligro abstracto no puede ser el modo de solucionar un problema de imputación objetiva, ni tampoco resulta muy claro que este tipo de modalidades tenga en realidad bien jurídico.

Entendemos, y solo sirve para complicar aún más la cuestión, que se debe distinguir, con J. Schulenburg[79], entre bien jurídico y objeto del bien jurídico. Si una conducta lesiona o pone en peligro algún elemento u

[76] R. Castillo Felipe, S. Tomás Tomás, *Proceso penal e inteligencia artificial: reflexiones en torno a su futura aplicación en la fase de juicio oral*, en esta obra, § 1.

[77] Peris Riera. *Inteligencia Artificial y neurociencias: Avances del derecho penal contemporáneo*, en esta obra, § 1.

[78] Si se considerase que la activación del algoritmo permite acreditar el concreto riesgo para el bien jurídico.

[79] Como considera el autor J. Schulenburg, *Relaciones dogmáticas entre bienes jurídicos, estructura del delito e imputación objetiva*, en *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho Penal o juego de abalorios dogmático?* (Dir. R. Hefendehl, A.V. Hirsch, W. Wohlers), Marcial Pons, Madrid, 2016, pp. 341-354.

objeto del bien jurídico (por tanto, algo tangible o preciso y determinado) no es necesario el delito de peligro abstracto, siendo suficiente con el delito de resultado o de peligro concreto; y al contrario, cuando lo que se pretende proteger no es un elemento u objeto concreto del bien jurídico, ni el bien jurídico en sí considerado puede ser entendido como individual sino como colectivo, es cuando procedería establecer, en este contexto temático, el delito como de peligro abstracto. Por ello, se decía más arriba que el legislador debe decidir, antes que nada, si la ciberseguridad, se ha convertido en un bien jurídico autónomo y colectivo (huyendo de *conceptos ideales e inatacables*, como destaca Hefendehl[80]) y, que fundamentará su protección más allá del concreto ataque a un bien jurídico individual o elemento individual concreto de un bien jurídico más colectivo. En este caso, se podrían tipificar tres conductas; una, de resultado pluriofensivo; otra, de peligro concreto y otra de peligro abstracto. Con ello se propiciaría la sanción de la lesión como delito de resultado y la aplicación del delito de peligro (concreto) si no se produce resultado alguno, o con la conducta se ha producido un resultado, pero también riesgo para otros sujetos, en cuyo caso concurriría en concurso ideal[81] con el delito de resultado). El delito de peligro abstracto quedaría para conductas muy iniciales.

Entendemos que la solución pasaría por distinguir entre aquellos ataques a la ciberseguridad (como bien jurídico colectivo y pseudo abstracto), de aquellos otros que atentan contra bienes individuales (como el patrimonio, intimidad, etc.). En este segundo caso, resultaría suficiente con tipificar un delito de resultado o peligro concreto (en términos muy parecidos a como se hace en la actualidad en los casos citados, y siendo el fenómeno tecnológico un medio comisivo específico).

No obstante, y aunque profundizar en ello excedería de un trabajo de esta naturaleza, de quedar reguladas ambas modalidades (resultado y peligro concreto para los casos de bien jurídico individual y peligro abstracto para los de bien jurídico colectivo), se podría interpretar que el delito de peligro abstracto no sería más que una tentativa del delito de resultado (habrá quien sugiera, incluso, que no es más que un acto preparatorio), lo que podría hacer innecesaria su tipificación, por redundante, para evitar problemas

[80] R. Hefendehl, *Las jornadas desde la perspectiva de un partidario del bien jurídico*, en *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho Penal o juego de abalorios dogmático?* (Dir. R. Hefendehl, A.V. Hirsch, W. Wohlers), Marcial Pons, Madrid. 2016, p. 401.

[81] Si como consecuencia de la conducta solo se ha producido lesión del bien jurídico individual, sin haberse causado riesgo para otros sujetos, el delito de resultado absorbería el delito de peligro concreto, en virtud de lo dispuesto del artículo 8 del código penal español.

hermenéuticos de tipo práctico. En este caso, y teniendo tipificada una modalidad de resultado (o incluso de mera actividad, pero lesivo), sería suficiente con la aplicación de los principios generales del código penal español (concretamente su artículo 16.1[82], para la tentativa (inacaba, en todo caso, para el delito de mera actividad), o el artículo 18 para los actos preparatorios), para valorar las distintas fases delictivas.

En cualquier caso, alejar al operador de interpretaciones creativas y de moda, impediría la absolución por falta de prueba respecto del riesgo concreto (hecho éste que será habitual), lo que es más propio de los delitos de peligro abstracto. Como señala S. MIR PUIG[83] lo que no podría admitirse es que en los delitos de peligro abstracto falte el tipo siempre que se pruebe que a posteriori no resultó peligro concreto, añadiendo que esto contradiría el fundamento político-criminal de los delitos de peligro abstracto, que ha de verse en la conveniencia de no dejar a juicio de cada cual la estimación de la peligrosidad de acciones que con frecuencia son lesivas (peligro estadístico).

Incluso, y si, como decimos, se planteara el legislador un bien jurídico autónomo colectivo y difuso, no extrañaría que se decantara por la fórmula del delito obstáculo, esto es, y como ha relatado la jurisprudencia del Tribunal Supremo, aquel fenómeno de criminalización anticipada mediante el que se castigan conductas en un momento anterior a la lesión del bien jurídico e incluso con anterioridad a que se genere un peligro concreto o abstracto para el bien jurídico. Son por lo tanto delitos que se configuran como auténticos obstáculos que tienen como función impedir que lleguen a producirse los actos delictivos futuros que se tipifican en otros preceptos. En ellos el principio de ofensividad cede ante la necesidad de prevención general y se presentan como tipos penales formales o de mera desobediencia mediante los que se anticipa, si bien en algunos casos de forma muy cuestionable, la barrera defensiva que supone la aplicación de toda norma penal (STS 2315/2017[84]). En realidad, y como señala P. Cuesta Pastor[85], la utilización por el legislador del delito obstáculo equivale a la criminalización de los actos preparatorios para cometer ciertos delitos.

[82] Donde se regula la tentativa del delito.

[83] Mir Puig, *Derecho Penal. Parte General*, p. 241.

[84] STS 2315/2017, de 8/6/2017 (ECLI: ES:TS:2017:2315), p. 6.

[85] P. Cuesta Pastor, *Delitos obstáculo. Tensión entre política criminal y teoría del bien jurídico*, Editorial Comares, Granada, 2002, p. 44.

6. *Conclusión*

Resulta difícil mantener una conclusión cerrada y definitiva (y no provisional) en una temática tan cambiante como es la ciberdelincuencia. En la actualidad, la solución que entendemos correcta pasaría por aceptar una de estas tres propuestas y que se exponen de manera esquemática:

En primer lugar, seguir entendiendo que lo informático es solo un medio comisivo específico y, por tanto, seguir regulando la cibercriminalidad como mera modalidad agravada dentro de las categorías tradicionales de delito (es lo que ocurre con la estafa, los daños, la intimidad etc.). Sin embargo, debemos tener en cuenta que el uso de la tecnología empieza a generar una realidad que merece ser tipificada de manera específica.

Por ejemplo, si una injuria se comete a través de cualquier aplicación conocida en la red (Twitter, Facebook, Instagram, …), se produce un *efecto eco* que está buscado de propósito por el autor. Este hecho es un claro elemento subjetivo del tipo que añade un plus de antijuridicidad a la conducta que requiere un tratamiento jurídico diferenciado. El derecho al olvido ni tan siquiera es capaz de eliminar este efecto eco. Es algo más que la mera publicidad[86], es la imposibilidad de que la conducta cese, porque siempre habrá un rastro visible del atentado al honor.

Como se ha señalado, y hacemos nuestro, los buscadores se encargan de sacar a luz dichos contenidos, una y otra vez, bajo un mismo principio: la libertad de expresión y de circulación de contenidos online aplicable a una internet que, según algunos, se autorregula y no requiere legislación (F. Tomeo[87]). Sin embargo, la experiencia demuestra la necesidad de poner límites a esta actividad. El problema es cómo hacerlo, sin que suponga merma de otros derechos. Se ha de partir del principio general de que no existe en la realidad (y tampoco, por tanto, en la red) un derecho al insulto.

En segundo lugar, crear un título autónomo en el que el legislador trate de manera conjunta el fenómeno de la cibercriminalidad, con la posibilidad incluso de establecer disposiciones comunes. Se trataría de trasladar los tipos actuales que regulan lo informático (que se convertirían así en delitos pluriofensivos) más los nuevos específicos que deben ser tipificados, con el consiguiente problema de sistematización. Esta posibilidad procede si se considerara que la seguridad en el ciberespacio tiene entidad autónoma

[86] El artículo 211 del código penal español establece que la calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

[87] F. Tomeo. *Calumnias e injurias on line*, en *Cibercrimen II* (Dir. D. Dupuy), B de f, Buenos Aires, 2018, p. 111.

y suficiente, como para erigirse en bien jurídico protegido independiente. Esta independencia nos permitiría configurar la ciberseguridad como un bien jurídico colectivo y permitiría establecer, en determinadas condiciones, delitos de peligro abstracto o, incluso, delitos obstáculo.

Entiendo que establecer esta modalidad típica[88] para resolver problemas de imputación objetiva sería pervertir los principios esenciales del derecho penal, dado que se estaría ocultando, a través de estas nuevas figuras legislativas, un claro y reprobable delito de sospecha como objeto de castigo. Allá donde haya un bien jurídico individual, sin posibilidad de considerarlo colectivo, precisa de la creación de delitos de resultado o, a lo sumo, de peligro concreto (donde el efectivo riesgo se convierte, en un elemento más del delito).

Y, en tercer lugar, establecer una circunstancia modificativa de la responsabilidad (agravante) con el fenómeno cibernético, de tal forma que el libro II no deba, salvo excepciones, regular de manera autónoma y específica cada una de las modalidades delictivas en las que quepa imaginar la cibercriminalidad. El problema que habría que analizar es la proporcionalidad de la pena, porque en muchas ocasiones la mera agravante no satisface la proporcionalidad de la pena en determinados delitos.

Todas las posibilidades se encuentran abiertas y son claramente mutables por otras, dependiendo, en mi opinión, de que el avance de la técnica permita dos cosas básicamente: De un lado, demostrar que el fenómeno cibercriminal es un hecho que no puede adaptarse a figuras tradicionales (salvo en supuestos específicos); y de otro, determinar con exactitud y precisión quién hay detrás del algoritmo, y probar que el derrotero seguido por éste es perfectamente conocido por su autor, al margen de que la víctima sea o no determinada desde un inicio. Esto, que hoy no ocurre, porque no hay medios que lo permitan (al menos medios directos que sean aptos para su prueba en un procedimiento penal) es lo único que permitiría tratar el ciberdelito, en todos sus aspectos, como delitos de resultado (o, en el peor de los casos, de peligro concreto), y no tan solo de las siempre discutibles figuras de peligro abstracto y obstáculo.

Con todo, el estudio caso a caso es imprescindible, y habrá de cuestionarse en cada modalidad delictiva la mejor opción, en función de los datos empíricos contrastados y sus resultados en un procedimiento judicial. Una vez queden resueltas las consideraciones de principios en derecho penal, restará entrar a detalle en la llamada parte especial, donde la solución se deberá hacer depender de otros factores más concretos y perfilados.

[88] Delitos de peligro abstracto.

En definitiva, estamos ante un nuevo fenómeno en el que, de momento, es mejor formular preguntas que respuestas categóricas, y entender que el vocabulario (los anglicismos) no construye teorías, solo distrae del problema central que sigue sin tener estructura ni solución.

7. *Bibliografía*

Agustina J.R., *Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización*. «Cuadernos de política criminal». Segunda época. Madrid. Núm. 136, Mayo 2022.

Beck U., *Sociedad de riesgo. Hacia una nueva modernidad*, Paidós, Barcelona-Buenos Aires-México, 2002.

Benítez Ortúzar I., *Ciberdelitos. la implementación en el ordenamiento interno de los acuerdos internacionales en materia de ciberdelincuencia*, en *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0* (Coord. M.J. Cruz Blanca/I. Lledó benito), Dykinson, Madrid, 2021.

Bonfante P., *Corso di diritto romano*, Giuffrè, Milano, 1963.

Cámara Arroyo S., *Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente*, en «Derecho y Cambio Social», Núm. 60, Abril-junio 2020.

Castillo Felipe R., Tomás Tomás S., *Proceso penal e inteligencia artificial: Reflexiones en torno a su futura aplicación en la fase de juicio oral*, en esta obra.

Cobo del Rosal M., Vives Antón T., *Derecho Penal. Parte General*, Tirant lo Blanch, Valencia, 1991.

Corvalán, J.G, *Presentación: Inteligencia artificial. Automatización y predicciones en el Derecho*, en *Cibercrimen III* (Dir. D. Dupuy/J.G. Corvalán), B de f, Buenos Aires, 2020.

Cuesta Pastor P., *Delitos obstáculo. Tensión entre política criminal y teoría del bien jurídico*, Editorial Comares, Granada, 2002.

Cumbreras M., López P., *¿Es necesario un marco ético para guiar el desarrollo y uso de la inteligencia artificial en las organizaciones?*, en *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0* (Coord. M.J. Cruz Blanca/I. Lledó Benito), Dykinson, Madrid, 2021.

De la Mata Barranco N.J., *Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 97 CP). El concepto de de*

privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación, en «Cuadernos de política criminal», segunda época, Núm. 118, mayo 2016.

Eduardo Aboso G., *Derecho Penal Cibernético. La cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación*, B de f, Buenos Aires, 2017.

Giraldi A., *Deshumanizando la culpabilidad: los sistemas inanimados en la teoría del delito*, en esta obra.

Garat S., Reale J., *La reforma penal en materia de cibercrimen en la República Argentina*, en *Cibercrimen II* (Dir. D. Dupuy), B de f, Buenos Aires, 2018.

González Tapia M.I, *Neurociencias e imputabilidad: recapitulando*, en esta obra.

Hefendehl R, *Las jornadas desde la perspectiva de un partidario del bien jurídico*, en *La teoría del bien jurídico ¿Fundamento de legitimación del derecho penal o juego de abalorios dogmático?* (Dir. R. Hefendehl, A.V. Hirsch, W. Wohlers), Marcial Pons, Madrid, 2016.

Hernández Díaz L., *El delito informático*. «EGUZKILORE, Cuaderno del Instituto Vasco de Criminología», 23, diciembre 2009.

Jakobs G., *Concurrencia de riesgos: curso lesivo y curso hipotético en el Derecho penal*, en «El Derecho Penal Lecciones y Ensayos», Nº 54, 1990.

H. Jescheck, T. Weigend, *Tratado de Derecho Penal. Parte General* (trad. M. Olmedo Cardenete), Comares, Granada, 2002.

Kurzweil R., *The Age of lntelligent Machines*, MIT Press, Cambridge, 1990.

Linfante Vidal I., *La relevancia de la previsibilidad jurídica*, en «DOXA, Cuadernos de Filosofía del Derecho», edición especial, 2017.

Lledó Benito I., *Ciberseguridad Versus Ciberdelincuencia*, en *El derecho penal, robots, IA y cibercriminalidad: desafíos éticos y jurídicos ¿Hacia una distopía?*, Dykinson, Madrid, 2022.

Mata y Martín R.M., *Criminalidad informática: una introducción al cibercrimen*. «Actualidad Penal», Núm. 37, Sección Doctrina, Semana del 6 al 12 Oct. 2003, Ref. XXXVI, tomo 3.

Martínez Atienza G., *El blanqueo de capitales y su sanción administrativa y penal*. «Revista de Derecho vLex», número 202, Marzo 2021.

Maté Jiménez C., *Big data. Un nuevo paradigma de análisis de datos*, en «Anales de mecánica y electricidad», noviembre-diciembre 2014.

Mir Puig S., *Derecho Penal. Parte General*, Reppertor, Barcelona, 2012.

Morán Blanco S., *La ciberseguridad y el uso de las tecnologías de la*

información y la comunicación (tic) por el terrorismo, en «Revista Española de Derecho Internacional». Sección ESTUDIOS. Vol. 69/2, julio-diciembre 2017.

Morillas Fernández D.L., *Implicaciones de la inteligencia artificial en el ámbito del derecho penal*, en esta obra.

Muñoz Alonso A., *Andamios para las ideas*. Colección Aula de ideas, volumen 1, Aula, Madrid, 1952.

Palma Herrera, J.M. *Inteligencia artificial y neurociencia. Algunas reflexiones sobre las aportaciones que pueden hacer al Derecho Penal*, en esta obra.

Palma Ortigosa A., *Decisiones automatizadas y protección de datos*, Dykinson, Madrid, 2022.

Pérez-Arias J., *Sistema de atribución de responsabilidad penal a las personas jurídicas*, Madrid, 2014.

Pérez-Arias J., *Cibercriminalidad: hacia la nueva realidad -virtual- del derecho penal*, en «Revista Internacional de Doctrina y Jurisprudencia», volumen 26, 2021.

Peris Riera J., *Inteligencia Artificial y Neurociencias: Avances Del Derecho Penal Contemporáneo*, en esta obra.

Perozzi S., *Istituzioni di Diritto Romano*, Milano, 1947.

Radbruch G., *Einführung in die Rechtswissenschaft*, Quelle & Meyer, Stuttgart, 1929.

Rayón Ballesteros M.C., Gómez Hernández J.A., *Cibercrimen: particularidades en su investigación y enjuiciamiento*, en «Anuario Jurídico y Económico Escurialense», XLVII, 2014.

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

Russel S., Norvig P., *Inteligencia artificial. Un enfoque moderno*, Pearson, Madrid, 2008.

Salvador Carrasco L., *Redes de anonimización en internet: cómo funcionan y cuáles son sus límites*, en «Revista de Instituto Español de Estudios Estratégicos», número 16/12. 2012.

Schulenburg J., *Relaciones dogmáticas entre bienes jurídicos, estructura del delito e imputación objetiva,* en *La teoría del bien jurídico ¿Fundamento de legitimación del derecho penal o juego de abalorios dogmático?* (Dir. R. Hefendehl/A.V. Hirsch/W. Wohlers), Madrid, 2016.

Souza de Menezes, C., Agustina J.R., *Big Data, inteligencia artificial y policía predictiva*, en *Cibercrimen III* (Dir. D. Dupuy/J.G. Corvalán), B de f, Buenos Aires, 2020.

Tamarit Sumalla J.M., *Ciberdelincuencia y cibervictimización*, en «Revista

de los Estudios de Derecho y Ciencia Política», n.º 22, Junio, 2016.
Temperini M., *Delitos informáticos y cibercrimen: Alcances, conceptos y características*, en C*ibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet*, Erreius, Buenos Aires, 2018.
Tomeo, F. *Calumnias e injurias on line*, en *Cibercrimen II* (Dir. D. Dupuy), B de f, Buenos Aires, 2018.