# Recensión del libro de Javier Valls Prieto, *Inteligencia artificial, Derechos Humanos y bienes jurídicos*

### Juan José González Rus

Universidad de Córdoba

GONZÁLEZ RUS, JUAN JOSÉ. Recensión del libro de Javier Valls Prieto, *Inteligencia artificial, Derechos Humanos y bienes jurídicos. Revista Electrónica de Ciencia Penal y Criminología.* 2022, núm. 24-r2, pp. 1-10

http://criminet.ugr.es/recpc/22/recpc24-r2.pdf

RESUMEN: Los estudios sobre inteligencia artificial en materia penal se han basado en el análisis de la responsabilidad penal por daños de las máquinas sin abordar todo el espectro de incidencia en los bienes jurídicos penales. Esta obra enfoca de forma original el análisis de los bienes jurídicos afectados por el uso de la inteligencia artificial aportando una metodología de análisis que facilité al jurista el análisis de la responsabilidad. Partiendo de una definición legal de inteligencia artificial con la que se delimita el marco de actuación, se basa en el análisis de casos ya documentados en los que la inteligencia artificial afecta a los derechos fundamentales de los individuos. Este estudio parte de los principios éticos comunes a las guías éticas más importantes para, desde un punto filosófico moral, determinar qué bienes jurídicos son los afectados. El resultado del estudio es que no es sencillo determinar los bienes jurídicos porque va a depender de qué tipo de tecnología se va a aplicar, en qué contexto y por quién. Para solucionar este problema el autor aporta una metodología de análisis y prevención de riesgos acorde con la normativa europea sobre inteligencia artificial.

PALABRAS CLAVE: Inteligencia artificial, Derechos fundamentales, Principios éticos, Bienes jurídicos.

TITLE: Review of the book by Javier Valls Prieto, Inteligencia artificial, Derechos Humanos y bienes jurídicos

ABSTRACT: Studies on artificial intelligence in criminal matters have been based on the analysis of criminal liability for damages caused by machines without addressing the whole spectrum of incidence on criminal legal goods. This work takes an original approach to the analysis of the legal goods affected using artificial intelligence, providing a methodology of analysis that facilitates the jurist's analysis of the liability of artificial intelligence. Starting from a legal definition of artificial intelligence that delimits the framework of action, it is based on the analysis of documented cases in which artificial intelligence affects the fundamental rights of individuals. This work starts from the ethical principles common to the most important ethical guides to determine, from a moral philosophical point of view, which legal goods are affected by artificial intelligence. The result of the study is that it is not easy to determine the legal assets because it will depend on what type of technology is going to be applied, in what context and by whom. To solve this problem, the author provides a methodology for risk analysis and prevention in accordance with European regulations on artificial intelligence.

KEYWORDS: Artificial intelligence, Fundamental rights, Ethical principles, Legal goods.

Fecha de recepción: 15 mayo 2022

Fecha de publicación en RECPC: 27 agosto 2022

Contactos: fd1goruj@uco.es - jvalls@ugr.es

SUMARIO: I. Enfoque general del libro. II.La inteligencia artificial. III. Supuestos de riesgo. IV. Principios éticos. V. Intervención penal. Referencias.

# I. Enfoque general del libro

Debo comenzar este breve comentario a la obra del profesor Valls Prieto, felicitando a su autor por su publicación. Se trata de un libro maduro, de quien conoce muy bien la magnitud de lo que trata y que desborda con mucho la pretensión inicial del autor, confesada expresamente, y que no sería otra que la de poner sobre la mesa determinadas preguntas, para algunas de las cuales reconoce también que no existe respuesta. Estimo, sin embargo, que el libro es bastante más que eso y constituye un paso más del profesor Valls Prieto en su brillante trayectoria en esta materia, que viene a sumarse a trabajos anteriores de gran calidad e interés.

Al leer el libro debo confesar que me han venido a la cabeza tiempos pasados, los años ochenta del siglo XX, cuando publicaba —todavía en tiempos del ¿ordenador? ZX Spectrum; aunque ya se adivinaba el amanecer de un mundo nuevo— mi temprana "Aproximación a los ilícitos patrimoniales relacionados con medios o procedimientos informáticos"; tema que fue calificado sin ambages por algunos ilustres penalistas del momento como una atrevida excentricidad más propia de la ciencia ficción que de la Ciencia del Derecho penal. A diferencia de entonces, hoy nadie sensato se atrevería a cuestionar la extraordinaria relevancia de la inteligencia artificial, la magnitud y complejidad de las cuestiones penales que suscita y, consecuentemente la utilidad e interés de la obra del Prof. Valls Prieto.

Por añadidura, el enfoque de aquel primer trabajo mío está en la línea del que se utiliza ahora en este excelente estudio: (i) exponer y valorar la significación social, jurídica y penal de la nueva tecnología; (ii) identificar los peligros para derechos humanos y bienes jurídicos penalmente relevantes; (iii) analizar las posibilidades de tutela que las figuras penales vigentes ofrecen frente a los riesgos detectados, y (iv) finalmente, señalar las carencias que se presentan y avanzar la forma de remediarlas.

En las "engañosas" 142 páginas del libro —que con una tipografía más generosa y cómoda para el lector serían, como poco, el doble—, se ocupa, con claridad, con rigor, desde fundamentos sólidos, de las cuestiones centrales que el tema plantea: (i) concepto de inteligencia artificial; (ii) ámbitos públicos y privados en los que está siendo utilizada habitualmente y riesgos que entraña; (iii) impacto de la misma en los derechos humanos; (iv) principios éticos sobre su diseño y aplicación elaborados por instancias nacionales e internacionales; (v) protección de los derechos fundamentales afectados; (vi) identificación de las figuras delictivas disponibles para la protección de los bienes jurídicos eventualmente amenazados por la sedicente inteligencia artificial y términos de la protección que son capaces de ofrecer, y (vii) conclusiones

<sup>&</sup>lt;sup>1</sup> GONZÁLEZ RUS 1986, pp. 107-164.

sobre las eventuales lagunas y reformas. Exactamente, a mi juicio, lo que el tema necesita.

# II. La inteligencia artificial

El obligado punto de partida, como no podía ser de otra forma, es la definición de inteligencia artificial, asunto en el que el autor nos muestra, sobre todo, la indefinición que caracteriza a los intentos más conocidos, la mayoría formulaciones circulares, que acaban identificando a la inteligencia artificial con el comportamiento "inteligente" de determinados sistemas o máquinas. Lo notable, empero, es que el autor, con gran sentido común, no se anima a añadir una noción propia, limitándose a señalar las características más relevantes para su tratamiento jurídico y marcando las diferencias inteligencia biológica y la inteligencia artificial. Y es que la inteligencia, humana o artificial, es más fácil de describir que de definir.

Aunque la interesada generalización del nomen "inteligencia artificial" encierra la sugerencia de que estamos ante una inteligencia "como la humana", ese parangón, estimo, está todavía lejos y las diferencias entre ambas son muchas; incluso si pretende referirse sólo a actividades específicas. La inteligencia biológica entraña facultades de la mente que permiten aprehender directa y espontáneamente datos e informaciones de todo tipo (materiales e inmateriales), interpretarlos, fijarlos como conocimiento concreto o abstracto, entender, razonar, formular y manejar conclusiones y abstracciones sobre la realidad, decidir con creatividad y sentido crítico, planificar, resolver problemas, aprender de la experiencia. Opera con lo racional y con lo irracional, gestiona emociones, puede dirigirse conscientemente a resultados funcionales y disfuncionales, preferir el mal al bien como resultado de la toma de decisiones, tiene sentido del humor, incluso. Por añadidura, tiene una dimensión de globalidad que no es planteable (todavía) en la denominada inteligencia artificial. Como resalta el autor, la inteligencia artificial es incapaz de manejar lo imprevisto o adivinarlo o crear algo de la nada, lo que la hace incapaz de actuar de forma efectiva ante situaciones completamente nuevas. Y, en lo que se refiere específicamente al análisis jurídico, añade el Prof. Valls, hay que descartar "cualquier intento de equiparar las acciones de los humanos con las de los sistemas inteligentes por muy eficaces que puedan ser". Hoy por hoy, concluye, no existe un sistema inteligente capaz de reaccionar como un humano, "aunque puede realizar tareas humanas con mayor eficacia".

La denominación de "inteligencia artificial", sin embargo, se ha convertido en un eslogan taquillero que se aplica a prácticamente todo lo quiera hacerse apreciar en el mercado: desde el más sencillo ingenio mecánico o electrónico regido por software, incluso básico, hasta los sistemas computacionales de la más alta complejidad. Ni el propio autor ha conseguido sustraerse a la seducción del término y apela

efectivamente en el título de su obra a la "Inteligencia artificial"; por más que ya desde las primeras páginas advierta que, en realidad –siguiendo a las más recientes propuestas de la Unión Europea–, debe hablarse de "sistemas de inteligencia artificial".

Las consecuencias inmediatas que lo anterior tiene para el tratamiento jurídico de la sedicente inteligencia artificial son, como destaca el autor, de gran relieve. En términos de responsabilidad, en la medida en que la inteligencia artificial es (todavía) una herramienta creada por personas, con patrones de actuación definidos por humanos, que por las decisiones y actos del sistema responderán las personas físicas que lo controlen. Como por otra parte se propone que sea y siga siendo en las declaraciones éticas sobre sistemas de inteligencia artificial. Así, por citar un solo caso, en las Directrices Éticas de la Comisión Europea (2019), estableciendo que los sistemas de inteligencia artificial no "deben tomar decisiones autónomas sin el control por parte de un humano". Aunque es evidente que el camino pretendido por algunos partidarios de la normativización absoluta de las categorías penales deja a un paso el reconocimiento a los sistemas de inteligencia artificial de la capacidad de responsabilidad penal autónoma, en la medida en que su diseño y funcionamiento queda obligado por deberes cada vez más definidos.

Otra cosa será en un futuro más o menos próximo, cuando el desarrollo de los sistemas cuánticos y, sobre todo, el aprovechamiento pleno de las sinergias entre tecnologías hoy todavía en desarrollo, permitan una capacidad de almacenamiento de datos y de procesamiento capaz de establecer interrelaciones semejantes a las que desarrolla el sistema neuronal propio de la inteligencia biológica. En ese contexto tecnológico, culminación plena del ensueño determinista, podrá conocerse y descifrarse el universo de factores e interacciones de la red neuronal en que se soporta y genera la inteligencia biológica, y, consecuentemente, las claves del comportamiento individual, resultando, en cuanto conocido, un proceso replicable en sistemas o máquinas electrónicas; momento en el que podrá hablarse propiamente de "inteligencia artificial", que podría conllevar, según el pronóstico, de algunos, el ocaso de la inteligencia biológica<sup>2</sup>.

### III. Supuestos de riesgo

La obra se ocupa a continuación de estudiar "supuestos de riesgo" para los derechos humanos sobre la base de las experiencias conocidas relacionadas con sistemas automatizados de toma de decisiones (pp. 27 a 44). En este ilustrativo apartado se da noticia y se describen las características y los resultados obtenidos con la utilización de la sedicente inteligencia artificial tanto en el sector público como en el privado. Se muestra con ello la dimensión real del problema, abarcando experiencias que van

<sup>&</sup>lt;sup>2</sup> GONZÁLEZ RUS 2020, pp. 177-186.

desde el campo de la medicina a la administración de justicia, pasando por la concesión de ayudas sociales, atención de indigentes, digitalización de la administración, selección y contratación de personal, estimación del rendimiento laboral, búsqueda de webs y posicionamiento en red, valoración de personas, servicios e instituciones en redes sociales, elaboración de perfiles sociológicos, fidelización de clientes, publicidad personalizada, determinación de precios, concesión de seguros, valoración de riesgos en el sistema financiero... Incluso más, puesto que, en el ámbito electoral, por ejemplo, ya se ha pasado del tratamiento de datos, personalización de mensajes y targeting electoral, a la manipulación directa del comportamiento del elector, como ocurrió en las campañas del Brexit y en las primeras elecciones norteamericanas de Trump, de la mano en ambos casos de Cambridge Analytica<sup>3</sup>. Lo que muestra un panorama que, aún completo, constituye, sin embargo, una mera avanzadilla de lo que está por llegar; dando, por cierto, mayor relevancia al tema que nos ocupa.

Se resaltan en la obra los riegos comunes de la inteligencia artificial y que tienen que ver fundamentalmente con la recolección y el tratamiento de datos, en condiciones que a menudo suponen una abierta lesión de la intimidad, con escaso o nulo control por el titular de la corrección de los mismos, y, como consecuencia, de su utilización en perfiles individuales o en los algoritmos del sistema. Limitaciones agravadas por la ingobernable dinámica de transferencia de datos de unos operadores a otros o a corredores de datos, que de facto hacen ineficaz el derecho de corrección, puesto que las rectificaciones -de llegar a producirse-, no alcanzan a los datos ya transferidos, que, aún erróneos, siguen siendo los utilizados. Igualmente graves son los riesgos en relación con los algoritmos del sistema, que acaban reproduciendo sesgos discriminatorios basados en la raza, la pobreza, la falta de arraigo social y la presumible peligrosidad, con resultados erróneos, cuando no arbitrarios, que han tenido graves consecuencias para los sectores afectados. Para ser justos, no obstante, habría que añadir que tales sesgos no son una característica de la inteligencia artificial, sino, propiamente, de la humana, desde el principio de los tiempos y que parecen haber encontrado en las redes sociales -tan útiles, tan dañinas-, su hábitat más fecundo.

De todas las experiencias de las que se da cuenta en la obra, las que personalmente me despiertan mayor interés son las que tienen que ver la Administración de Justicia. En lo que se refiere al tratamiento de la información, como destaca el autor, no puede discutirse que los resultados son buenos y útiles. Como muestra de ello, se recuerda en la obra que "Watson" (IBM) aprobó en 2016 el examen de la abogacía norteamericana, que ya es decir bastante. Igualmente, se recuerda la importancia que para el sistema jurídico en su conjunto tienen los buscadores de jurisprudencia y de documentación legal, los analizadores inteligentes de sentencias, los métodos de resolución online de litigios, la elaboración de borradores de escritos y contratos, detección

<sup>&</sup>lt;sup>3</sup> GONZÁLEZ RUS 2022.

de cláusulas contradictorias, asesoramiento online de clientes, predicción de costos, cálculo de éxito probable de demandas o reclamaciones, elaboración de programas de cumplimiento...

Según se muestra en la obra, en la confección de decisiones judiciales los avances son más limitados y los resultados más inciertos; ni parece que puedan esperarse grandes mejoras a corto plazo, me permito añadir, mientras no se produzcan avances más sustanciales en el desarrollo de la inteligencia artificial. Las principales aplicaciones han tenido que ver en la prevención de la criminalidad, la evaluación de la peligrosidad y de la reincidencia (sistema norteamericano COMPAS, en la determinación de la posibilidad de reincidencia y aplicación de penas alternativas, y los sistemas HART, del Reino Unido, para evaluar el riesgo de reincidencia en base a archivos policiales, y Pred Pol, para el análisis de zona geográficas con elevados índices de criminalidad, entre otros), cuya aplicación ha sido puesta en entredicho por reproducir sesgos discriminatorios en sus resultados. En lo relativo a España se da noticia en el libro de la aplicación de programas de gestión de patrullas y de trabajo policial, con Vinfo Pol, Appolo (Policía Local), VeriPol (falsedad de denuncias en delitos contra la propiedad) y VioGen (necesidad de protección policial a víctimas de violencia de género); aunque no se comentan los resultados obtenidos con la aplicación de los mismos. El principal riesgo de estos sistemas, añado por mi parte, es que pueden consolidar inercias sobre las que ya advirtieran las teorías del "llabeling approach", incrementando la vigilancia, persecución y punición de sectores concretos de población asociados a la pobreza, la raza, la marginación, la educación o la cultura.

# IV. Principios éticos

La conciencia de los grandes riesgos que conlleva la aplicación de la sedicente inteligencia artificial para los derechos fundamentales y para los valores del propio sistema social ha provocado la elaboración de diversos principios éticos sobre su diseño y uso. En el libro se exponen y comentan los nueve documentos de mayor importancia en la materia, que, como se resalta, ofrecen un alto grado de coincidencia en lo fundamental (pp. 47 a 69).

Como resume el autor, puede concluirse que prácticamente todas las propuestas coinciden en el necesario respeto, en el diseño, creación, recogida de datos, elaboración de algoritmos e implementación y aplicación de los sistemas de inteligencia artificial, de básicamente ocho principios éticos que tienen que ver con el respeto a los derechos fundamentales, el protagonismo de la intervención humana, la seguridad de los sistemas de información, la salvaguarda de la privacidad y de la diversidad, la garantía de transparencia, la protección del medio ambiente, la no discriminación, la repercusión social beneficiosa de sus funciones y la rendición de cuentas.

Aunque hay diferencias en el desarrollo de los citados principios, que el autor advierte, básicamente el contenido que se asigna cada uno de ellos es semejante y se traduce en compromisos concretos de actuación también similares: garantía de la dignidad humana, proclamación de que la responsabilidad por los sistemas autónomos será de los humanos, principio de prudencia en el uso peligroso de los sistemas, prohibición de aceptar riesgos que dañen a seres humanos, eliminación de sesgos discriminatorios tanto en la elaboración de algoritmos como en la recogida de datos, garantía de los derechos del titular en la recogida y tratamiento de los datos personales, sostenibilidad de los sistemas, protección del medio ambiente, utilidad social de los resultados del sistema, trato justo de las necesidades y soluciones, transparencia de los sistemas (que permita la trazabilidad de los datos y de los procesos en que se apoya la decisión del sistema inteligente), elaboración de auditorías sobre algoritmos, datos y procesos, neutralidad en la proposición o valoración de estilos de vida individual o colectiva, etc.

En cuanto a la Carta de Derechos Digitales de España, se resalta que básicamente recoge los principios éticos de las declaraciones principales, aunque estima el Prof. Valls que no pasa de ser una recopilación de principios interpretativos y que no establece un marco claro para la inteligencia artificial. Destaca el autor la desaparición en la redacción final del documento de dos puntos que tienen singular interés. Uno, el reconocimiento del derecho de los usuarios a ser informados de que se comunican con sistemas de inteligencia artificial, garantizando en todo caso su derecho a reclamar ser atendidos por un humano. Otro, la prohibición del uso de sistemas de inteligencia artificial cuando su objeto sea manipular o perturbar la voluntad de las personas, en cualquier aspecto que afecte a los derechos fundamentales. Sería interesante saber el porqué de la desaparición de estos compromisos iniciales y si ello supone efectivamente o no una merma real en la protección de los derechos digitales de los ciudadanos.

### V. Intervención penal

De la exposición de lo ético se pasa a la incidencia de la inteligencia artificial en los derechos fundamentales, para concluir finalmente en la identificación de los bienes jurídicos que deberían ser penalmente protegidos (pp. 71 a 84). Ello es coherente con una estrategia global de control de los riesgos derivados del uso de la pretendida inteligencia artificial, que necesariamente ha de contar con mecanismos de control técnico, autorregulaciones, regulación y control administrativo y, en último término, intervención penal. El análisis lo sitúa el autor en seis áreas: sistema judicial, sistema financiero, sanidad, moderación de contenidos en web, recursos humanos y educación. En relación con cada uno de ellos se determina el impacto en los derechos fundamentales que tendría la aplicación de los sistemas automatizados de decisión, diferenciando entre impactos negativos positivos y efecto neutro.

Según el autor, hasta veinte derechos fundamentales se verían afectados por la inteligencia artificial (v. tabla resumen, p. 84), la mayoría de los cuales están incluidos en las declaraciones internacionales y europeas de derechos y en la Constitución española (salvo las excepciones que señala). Como principalmente afectados se coincide en señalar a la libertad y a la autonomía, la no discriminación, la privacidad, la no estigmatización, la intimidad, el secreto de las telecomunicaciones, la dignidad de la persona, libertad de expresión, transparencia y libre desarrollo de la personalidad. Aunque el informe del Consejo de Europa (2019) sobre la protección de los derechos fundamentales ante la inteligencia artificial, plantea la aparición de nuevos derechos y la necesidad de adaptaciones de derechos fundamentales existentes como consecuencia de la aplicación de sistemas automatizados de decisión.

Una vez identificados los derechos fundamentales relacionados positiva o negativamente con el uso de la inteligencia artificial se aborda el plano concreto de su desarrollo legislativo (pp. 85 a 106). Parco, por cierto, pues la única realidad tangible parece ser el art. 35 del Reglamento General de Protección de Datos, en el que se reclama la necesidad de realizar una evaluación de impacto en la privacidad.

Respecto de la intervención penal, y frente a lo que parece estimar el autor, creo que concurren las condiciones precisas para que la misma se produzca ya, sin necesidad de esperar a que se agoten las pretendidas cinco fases del proceso de criminalización, que, por otra parte, pueden darse por perfectamente cumplidas. Al fin y al cabo, para la legitimidad de la intervención basta con que concurran la premisa que señalara M.E. Mayer a principios del siglo XX: que haya un bien jurídico digno, susceptible y necesitado de protección. Y lo mismo debe valer para completar la protección de los ya protegidos frente a nuevas formas de agresión, como viene a ocurrir con la inteligencia artificial.

En cuanto a los términos concretos de la intervención penal, el autor aborda la cuestión, a mi juicio, desde premisas político criminalmente correctas: en primer lugar —sobre la base de lo anteriormente expuesto—, identificando los bienes jurídicos que pueden resultar afectados por el uso de la inteligencia artificial; después, comprobando hasta qué punto los tipos penales concernidos por esa tutela permiten la protección pretendida. El problema es muy parecido al que se planteó en su día con el desarrollo de las tecnologías informáticas y las redes de transmisión de datos, que alguna doctrina pretendió abordar con la creación de bienes jurídicos específicos—generalmente en términos de seguridad de sistemas o de funciones— para cuya protección se arbitrarían nuevas figuras delictivas—lógicamente, de peligro, preferiblemente abstracto— que habrían de configurar, llegó a decirse, un nuevo Derecho penal de la Informática. Personalmente nunca compartí este criterio, como he dicho en diversas ocasiones. Me parecía mucho más oportuno avanzar desde lo ya disponible, determinado las posibilidades de protección que ofrecía el Código penal, proponiendo fórmulas de complementación de los tipos penales vigentes—con objetos

materiales, conductas típicas, efectos y resultados específicos, e interpretaciones acordes con la singularidad del medio y entorno informático— y, después, si fuera necesario, llenar efectivamente las lagunas de protección que se apreciarán con las figuras delictivas nuevas que resultaran oportunas; incluso de peligro, naturalmente. Camino, por cierto, que fue el elegido por el Código penal español y es dominante en el derecho comparado.

Desde un enfoque semejante, y en relación con la inteligencia artificial, el Prof. Valls Prieto analiza el estado de la protección en relación con cada uno de los bienes jurídicos eventualmente amenazados por la inteligencia artificial, concluyendo que "las instituciones jurídicas que tenemos en la actualidad nos permiten tener una primera herramienta de defensa ante los errores/actuaciones de los sistemas inteligentes." "Muchos de los casos expuestos en el capítulo segundo de esta obra" —supuestos de riesgo— "pueden encontrar la adecuada protección mediante los derechos fundamentales, el sistema de responsabilidad civil y el Código penal."

En relación con vacíos de tutela y el eventual reconocimiento de bienes jurídicos nuevos, considera "que no se encuentran regulados todavía" temas centrales como la responsabilidad por el funcionamiento del sistema, la rendición de cuentas y el principio de transparencia, principios éticos sin acomodo en el Código penal, mostrando su simpatía por la posibilidad de dar reconocimiento al bien jurídico "confianza en el sistema jurídico en los bienes jurídicos colectivos" como se ha propuesto por algunos autores. Asimismo, respecto de la privacidad considera necesaria la creación de una "versión colectiva del bien jurídico privacidad", en la línea propuesta por otros autores.

Desde la perspectiva de los peligros que genera la inteligencia artificial, considera el autor que el Código penal protege suficientemente el bien jurídico discriminación y el derecho a la igualdad (art. 511, 314, 153.1 y agravante 22.4). No, en cambio, la "autonomía de las personas", la dignidad personal (sin protección directa), el derecho a la libertad de expresión en las redes y el derecho de reunión, y que respecto de la vida y la integridad física se hace necesaria una regulación "más fina", que incluya riesgos actualmente no contemplados. Semejantes carencias se producirían en relación con bienes jurídicos de significación económica (publicidad, protección del mercado, libre competencia, derechos de los trabajadores), también necesitados de reformas. En los delitos contra la administración de justicia y contra los derechos fundamentales echa en falta el castigo de la forma imprudente, que sería común en la utilización de sistemas inteligentes. Finalmente, en cuanto a la administración pública, analiza la eventual incidencia que la inteligencia puede tener en relación con los delitos de prevaricación, cohecho, tráfico de influencias, malversaciones, y delitos cometidos por los funcionarios, respecto de los que aprecia también carencias de protección que deberían ser corregidas.

Con todo, finalmente el autor se apunta también a la usual fórmula utilizada en

trances semejantes de que la revisión de los tipos o la creación de los específicos acabe "en lo que podríamos llamar un Derecho Penal de la máquina con un carácter especial y específico para este tipo de utensilios". Lo que no comparto, como ya he dicho antes, por mi natural desconfianza a la creación *ad hoc* de derechos penales específicos, irremediablemente impelidos a la autonomía, que pueden generar dinámicas interpretativas y jurisprudenciales propias y la pérdida de la unidad de interpretación y aplicación, conforme a postulados dogmáticos y legales comunes, que requiere el respeto al principio de igualdad y a la seguridad jurídica, tan esenciales en materia penal.

Desde el punto de vista estrictamente penal, es evidente que la última parte de la obra es la más sustancial. Aunque doy por sentado que las conclusiones del profesor Valls se soportan en un detallado análisis de los supuestos de riesgo y de las posibilidades actuales de tutela, creo —aquí sí— que el resumen que se incluye en el libro debería constituir el punto de partida para estudios más detallados y concretos que continúen la línea de investigación abierta tan brillantemente con trabajos anteriores, consolidada con este libro, y que pueden aportar mucho en el debate abierto en torno a la contemplación penal de la sedicente inteligencia artificial. Sobre todo, mirando a lo que el futuro puede traernos a medio plazo.

#### Referencias

- GONZÁLEZ RUS, J.J. (1986), "Aproximación a los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *Revista de la Facultad de Derecho de la Universidad Complutense*, Monográfico 12, pp. 107 y ss.
- GONZÁLEZ RUS, J.J. (2020), "El futuro del Derecho Penal", en De Remesal et al: *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Volumen II, Madrid, pp. 177–186.
- GONZÁLEZ RUS, J.J. (2022) ¿Nuevos retos para el Derecho Penal", en Libro Homenaje al Profesor Ignacio Berdugo Gómez de la Torre, en prensa.