3

RECENSIÓN DE LA OBRA *TECNOLOGÍAS ABUSIVAS Y DERECHO*, DIRIGIDO POR LOS PROFESORES FRANCISCO CAAMAÑO Y DANIEL JOVE VILLARES, EDITORIAL TIRANT LO BLANCH, VALENCIA, 2024

L. Irene González Martínez

Investigadora predoctoral
Universidad de A Coruña

El desarrollo tecnológico ha favorecido un nivel de progreso que sin él habría sido inimaginable. La generalización del acceso a internet supuso una suerte de democratización del acceso a la información, que nos permitió alcanzar nuevas cotas de conocimiento. El desarrollo de las redes sociales y aplicaciones de mensajería permitió una comunicación cada vez más inmediata y global, donde el número de receptores de la comunicación es de una magnitud nunca vista. Sin embargo, el cambio más significativo a nivel tecnológico ha llegado de la mano de la Inteligencia Artificial, una tecnología disruptiva con efectos transversales en todas las áreas del conocimiento y de la ciencia y que nos sitúa en un nuevo escenario tecnológico, productivo y social.

No obstante, a pesar de la importancia que revisten las posibilidades que abren estas nuevas tecnologías a todos los niveles, resulta extremadamente importante evaluar y prever los riesgos a los que pueden someternos, pues estamos ante herramientas que, usadas maliciosamente, tienen la potencialidad de causar daños de consecuencias catastróficas, poniendo en jaque la democracia y hasta a la propia humanidad.

La presente obra es uno de los resultados del grupo de investigación «Democracia y derechos en el entorno digital», formado por varios profesores del Área de Derecho Constitucional de la Universidad de A Coruña. En el seno de la investigación llevada a cabo por este grupo se organizó una Jornada sobre Tecnologías abusivas y derechos fundamentales en la Facultad de Derecho de la Universidad de A Coruña, en la que se dieron cita importantes académicos que ya se habían destacado por su estudio de la materia. Este libro colectivo recoge las ponencias presentadas durante esta Jornada junto con otras aportaciones que con las que se ha buscado dar una más completa cobertura a la materia objeto de estudio, incor-

porando perspectivas expertas en determinadas cuestiones de la tecnología en los derechos y su protección.

La obra aborda la difícil cuestión del impacto de las nuevas tecnologías y las tecnologías disruptivas sobre los derechos fundamentales, analizando especialmente si, en este ámbito tan cambiante, es suficiente la regulación existente para dar respuesta a las nuevas necesidades o si se hace necesaria una nueva regulación ajustada a los nuevos retos. Concretamente, se centra en siete aspectos clave: el derecho al entorno digital; las transformaciones culturales provocadas por los algoritmos; el Reglamento europeo de inteligencia artificial; las herramientas de reconocimiento facial; las inteligencias artificiales generativas; la neurotecnología y los neuroderechos y la ciberseguridad.

Inaugura el libro el profesor Francisco Caamaño analizando el derecho al entorno digital. Este derecho, construido por la jurisprudencia, nace como respuesta a la necesidad de proteger la «intimidad digital» en el caso del registro de dispositivos electrónicos y ha sido objeto de una importante evolución jurisprudencial que el profesor analiza en su trabajo de manera crítica y detallada. Plantea que el derecho al entorno digital, más que un derecho fundamental de nueva generación debe ser considerado como una garantía procesal, pensada no tanto para proteger a las personas de las posibles injerencias de los poderes públicos en sus esferas de privacidad constitucionalmente protegidas, como para validar la prueba conseguida a través de esas injerencias. Esto lleva al profesor a cuestionarse incluso la necesidad de este nuevo derecho concluyendo que: «la ecuación nuevas tecnologías *ergo* nuevos derechos, ni siempre es cierta, ni siempre es necesaria».

En el segundo capítulo Francisco Balaguer Callejón aborda la importante cuestión de cómo las nuevas tecnologías han modificado y siguen modificando nuestra sociedad cambiando nuestra percepción del espacio y del tiempo. En el nuevo ecosistema digital, como bien indica el autor, «cada individuo tendrá libertad para configurar su vida en el nivel de dependencia de las nuevas tecnologías que considere oportuno», sin embargo, resulta de gran importancia que el derecho vele por que el avance tecnológico sea compatible con los principios y valores constitucionales.

El profesor Balaguer ahonda en el cambio en la percepción del tiempo que ha tenido lugar debido a la generalización en el uso de internet y redes sociales, que permiten un acceso inmediato a la información —y desinformación— a la par que una interacción permanente que antes sólo era posible mediante una conversación telefónica. Uno de los principales problemas de esta inmediatez es que genera la ilusión de que todo puede o debe ser resuelto con esa celeridad, cuando hay procesos que necesariamente requieren un tiempo de debate y reflexión como, por ejemplo, los procesos políticos.

Continúa el autor analizando la modificación del espacio público generada por las redes sociales y aplicaciones de internet que, para contentar a un público global, recurren a algoritmos que les permiten segmentar a ese gran público para ofrecer a cada usuario sólo las opiniones que coinciden con las suyas propias, generando un efecto burbuja que aleja a las personas usuarias de la verdad fomentando así la

radicalización y el enfrentamiento y provocando, en definitiva, una situación de desinformación sistémica que se ve agravada por la irrupción de las inteligencias artificiales generativas.

La obra colectiva continúa con un trabajo de Miguel Ángel Presno Linera en el que realiza un pormenorizado análisis sobre el origen y desarrollo del Reglamento Europeo de Inteligencia Artificial. Así, capítulo tras capítulo, repasa orígenes y fundamentos de la regulación de la Inteligencia Artificial, para pararse después a analizar qué debemos entender por inteligencia artificial y cuáles son los principios generales aplicables a cualquier sistema de IA.

Se detiene a continuación el autor en el sistema de regulación basado en los riesgos adoptado en el reglamento, una concreción del principio de precaución que rige tanto en nuestro ordenamiento interno como en la Unión Europea y que lleva a regular los distintos sistemas de IA según el riesgo que supongan. Concluye el profesor Presno con una interesante reflexión final sobre la posibilidad, sin duda deseable, de que pueda generarse un «efecto Bruselas» que lleve a otros gobiernos a adoptar regulaciones semejantes fuera del ámbito de la Unión Europea.

La siguiente aportación llega de la mano de la profesora Mª Josefa Ridaura Martínez que dedica su trabajo a la tecnología de reconocimiento facial, una materia en la que la dicotomía seguridad vs privacidad alcanza su máxima expresión. Digitalizar supone hacer rastreable algo que no lo era y por ello analiza la profesora Ridaura si eventualmente puede resultar proporcional «vigilar a todos para controlar solo a algunos», especialmente teniendo en cuenta que ni siquiera los algoritmos pueden aportar una certeza absoluta, sino que están sujetos tanto al error estadístico, como a los sesgos discriminatorios derivados de los datos de entrenamiento.

Preocupa también a la profesora Ridaura el posible efecto amedrentador del reconocimiento facial, ya que el «saberse vigilados puede afectar de lleno a la libertad en general, y particularmente a la libertad de manifestación y de expresión». Por ello, entiende se hace necesaria una ponderación «ex ante» de los derechos que podrían entrar en conflicto tanto en la fase de diseño como en la implementación de este tipo de tecnologías. Destaca la ausencia de una normativa precisa y detallada sobre la materia, que regule con las debidas garantías el uso del reconocimiento facial más allá de la normativa sobre protección de datos o ciertas normas de «soft law» aprobadas hasta el momento.

Antes de terminar con una aproximación a la regulación de la materia en el Reglamento Europeo de Inteligencia Artificial, se detiene a estudiar el uso de los datos biométricos por las Fuerzas y Cuerpos de Seguridad del Estado, tanto con fines de investigación criminal como para preservar la seguridad, analizando de manera detallada la normativa aplicable y los requisitos para su utilización, que deberá estar sujeta al principio de proporcionalidad para proteger todos los derechos en juego.

El siguiente trabajo del libro colectivo, firmado por la profesora Ana Aba Catoira, aborda de manera exhaustiva la problemática de la regulación de la IA

generativa. Partiendo de la base de que los sistemas de IA suponen indudables ventajas en términos de eficacia, economía, desarrollo o bienestar, destaca que no pueden obviarse los riesgos que los mismos conllevan y que requieren de una regulación adecuada que garantice la protección de los derechos constitucionalmente protegidos.

No obstante, señala la profesora Aba que no se trata tanto de regular el uso de la tecnología en sí, como de regular de manera efectiva y adecuada determinados aspectos, específicamente en materia de transparencia, que hagan menos opacos los procesos de toma de decisiones automatizadas a través de una mayor transparencia en los algoritmos que permita una rendición de cuentas efectiva.

El capítulo continúa con un repaso de la evolución de la Inteligencia Artificial para después abordar el estudio de las principales respuestas legales ante esta tecnología, tanto a nivel internacional y nacional, como comunitario, prestando especial atención a la regulación de estos modelos en la propuesta de Reglamento Europeo de Inteligencia Artificial y al debate surgido en el proceso de tramitación en relación con los modelos de IA generativa o modelos fundacionales (modelos de propósito general). Un debate que culminó con la inclusión de estos modelos en la regulación del Reglamento Europeo a través de obligaciones de transparencia y colaboración que permitan a las personas usuarias tener suficiente información para poder cumplir con los requisitos de regulación.

El penúltimo capítulo del libro lo dedica el profesor Ángel María Judel Pereira al estudio de la neurotecnología y cómo esta puede afectar a la libertad de la persona y, por extensión, a los derechos humanos en general.

En su trabajo el profesor Judel repasa la evolución de la neurotecnología y las primeras respuestas ante los riesgos que la misma podía suponer, concretados en un primer momento en: privacidad y consentimiento, identidad, aumento de capacidades y equidad de acceso al mismo y la predisposición y manipulación de los procesos mentales.

Profundiza en este último riesgo haciendo una aproximación a los principales estudios publicados sobre neurotecnología en los que se prueba que se ha superado ya «una fase inicial de registro e interpretación de la actividad cerebral, para internarse en una nueva fase decodificativa y predictiva», una nueva fase en la que surgen nuevos riesgos a los que el ordenamiento debe dar respuesta. Y ello porque este tipo de tecnologías permiten no sólo el desarrollo de nuevas capacidades de los seres humanos y entidades artificiales, sino también «el desarrollo de nuevas formas de cibercrimen, de alteración de la realidad y de intervención sobre los procesos mentales y de privacidad de las personas».

Para dar respuesta a estos riesgos se formulan los neuroderechos, distinguiendo el autor entre los dos modelos existentes, el del profesor Rafael Yuste (que distingue cuatro neuroderechos distintos: derecho a la privacidad mental, el derecho a la identidad y a la toma de decisiones, derecho a un aumento cognitivo justo y derecho a la ausencia de sesgos) y el de los profesores Roberto Adorno y Marcello Ienca

(que condensan los neuroderechos en tres: privacidad mental, integridad mental y continuidad psicológica).

Continúa el profesor Judel analizando la regulación existente entre la que destaca el caso de la República de Chile, el único Estado que ha recogido expresamente en su Constitución la protección de la actividad neuronal, una norma que ya ha sido aplicada en una sentencia pionera en el caso Guirardi vs. EMOTIV, que también es objeto de análisis en este trabajo.

Para terminar, el autor plantea tres importantes conclusiones: 1) que los neuroderechos deben formar parte de los derechos humanos; 2) que el cerebro humano en sí mismo debe ser considerado como sujeto de derechos; y 3) que resulta necesario crear una nueva categoría reforzada de datos personales: los metadatos cerebrales.

El último capítulo del libro llega de la mano de la profesora Tamara Álvarez Robles, que dedica su aportación a la ciberseguridad, una materia complicada en la que no contamos siquiera con un concepto unívoco.

Ello lleva a la autora a dedicar la primera parte de su trabajo a definir el concepto de ciberseguridad desde tres enfoques distintos. En primer lugar, repasa las aportaciones de distintos organismos y las principales normas encargadas de la ciberseguridad que ofrecen una definición altamente técnica y en la que destaca el componente tecnológico-digital. En segundo lugar, deslinda el concepto de ciberseguridad de otras figuras relacionadas pero diferentes, como la seguridad de la información o la ciberdefensa. Por último, define la ciberseguridad como concepto genérico que «aborda la protección de activos de información ante amenazas que comprometen su procesamiento, almacenamiento y transporte en sistemas interconectados».

Los siguientes apartados de este capítulo analizan la regulación de la ciberseguridad en distintas normas. En primer lugar, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, cuyo artículo 82 se centra en garantizar la seguridad de las comunicaciones, una seguridad que depende por un lado de los proveedores, y por otro del Estado, sobre el que recae la obligación de garantizar este derecho para su ciudadanía, que simboliza la «seguridad integral, transversal y descentralizada».

En segundo lugar, repasa el marco normativo tanto europeo como nacional en materia de ciberseguridad destacando la regulación recogida en la Carta de Derechos Digitales que, si bien se trata de una norma no vinculante, en opinión de la profesora viene a corregir y/o complementar la Ley Orgánica 3/2018 de dos maneras: señalando explícitamente la necesidad de una colaboración supranacional y nacional, público-privada y con la sociedad para responder a los desafíos o conseguir garantizar la ciberseguridad de forma integral y, por otro lado, resaltando la necesidad de fomentar una cultura de ciberseguridad.

Para concluir, la profesora Álvarez Robles se refiere al Global Cybersecurity Index de la International Telecommunications Union (ITU), un índice que mide el compromiso de los países con la ciberseguridad y en el que España ha ido evo-

lucionando desde el puesto 30 (respecto de 196 estados) en 2015 hasta el cuarto puesto (respecto de 194) en 2020 lo que evidencia un importante progreso cuya consolidación depende, en opinión de la autora, de que la sociedad «adquiera plena conciencia y formación en materia de ciberseguridad».

En definitiva, estamos ante una obra que analiza con maestría las más importantes manifestaciones de las tecnologías disruptivas, los riesgos que las mismas pueden suponer y las posibles respuestas del derecho ante ellos. Se trata de una tarea compleja que es llevada a cabo por los diferentes coautores con gran rigor académico y científico, mostrando una gran capacidad expositiva y de síntesis, lo que arroja como resultado una obra colectiva completa y de gran claridad. Nos encontramos ante un trabajo necesario, que afronta sin ambages una materia de extraordinaria actualidad e importancia y que está llamado a convertirse en una obra imprescindible para el estudio de los retos normativos ante la nueva era digital.