

1 2 9 0



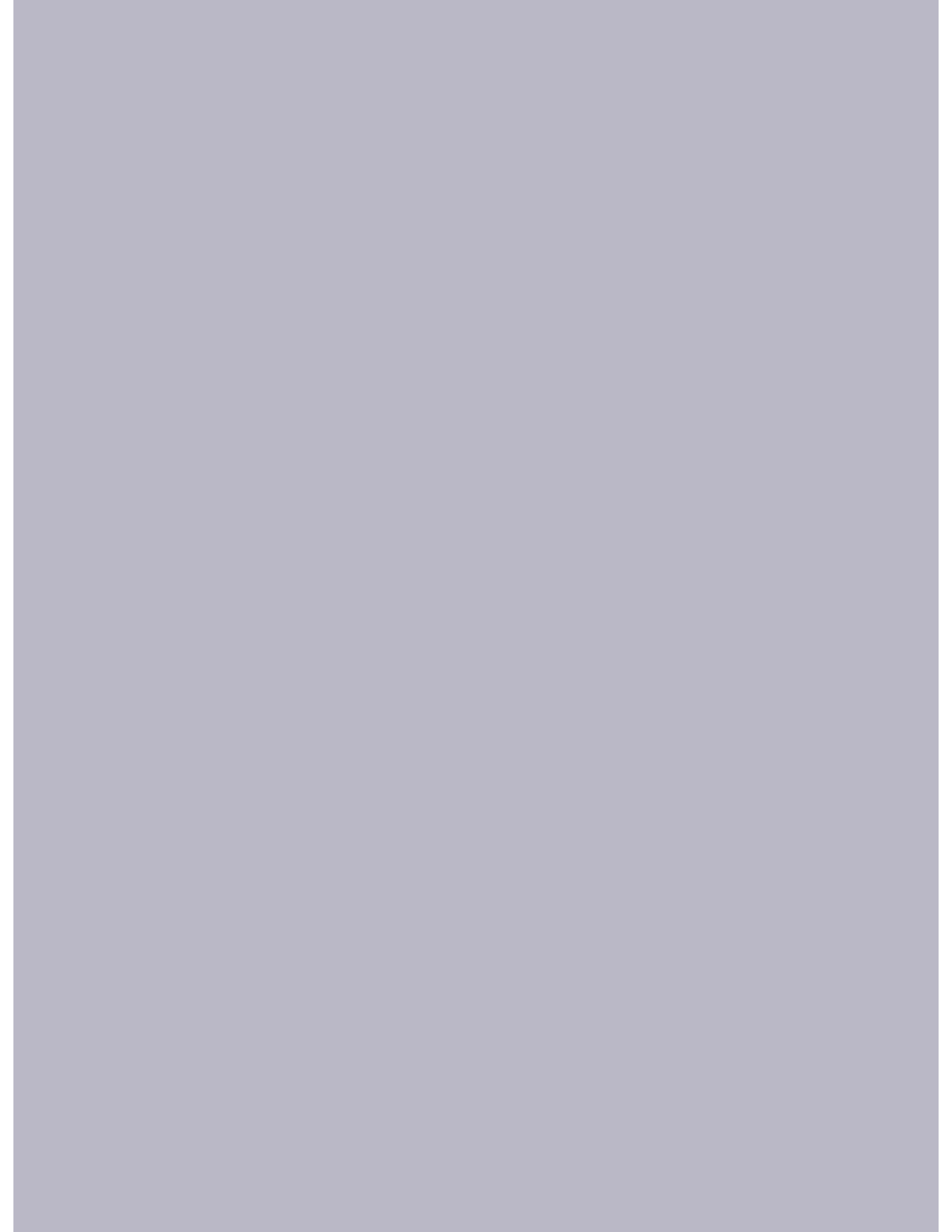
INSTITUTO JURÍDICO
FACULDADE DE DIREITO
UNIVERSIDADE DE
COIMBRA

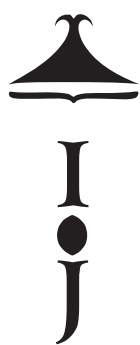
fct
UID04643
Fundação
para a Ciência
e a Tecnologia

Digital Transformation and Governance in the Judiciary

COORDENAÇÃO:

Fabício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell





Ficha Técnica

TÍTULO

Digital Transformation and Governance in the Judiciary

COORDENAÇÃO:

Fabício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell

EDIÇÃO

Instituto Jurídico
Faculdade de Direito da Universidade de Coimbra
geral@ij.uc.pt • www.uc.pt/fduc/ij
Colégio da Trindade • 3000-018 Coimbra

CONCEPÇÃO GRÁFICA

Pedro Bandeira

CAPA

Dalldesign

ISBN: 978-989-9075-92-4

e-ISBN: 978-989-9075-85-6

DOI: 10.47907/DigitalTransformationAndGovernance/livro

julho de 2025

A publicação do presente trabalho inscreve-se nas atividades do IJ/UCILeR (Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra), no contexto do projeto estratégico UID 04643 – Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra (financiado pela FCT – Fundação para a Ciência e a Tecnologia).

Fabrício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell
Editors

**Digital Transformation and Governance
in the Judiciary**

Authors

Ana Carla Werneck	Inês Oliveira
Audrey Kramy Araruna Gonçalves	Irene González Pulido
David Soto	Irene Yáñez García-Bernalt
Fabrício Castagna Lunardi	Lorenzo-Mateo Bujosa Vadell
Federico Bueno de Mata	Pedro Miguel Alves Ribeiro Correia
Fernando Martín Diz	Ricardo Pedro
Francesco Contini	Salomão Akhnaton Z. S. Elesbon

1 2 9 0



INSTITUTO JURÍDICO
FACULDADE DE DIREITO
UNIVERSIDADE DE
COIMBRA

University Of Coimbra
National School For Training And Improvement Of Judges (Enfam)

**ACADEMIC AND SCIENTIFIC COOPERATION BETWEEN THE FACULTY OF LAW OF
THE UNIVERSITY OF COIMBRA (FDUC) AND THE BRAZILIAN NATIONAL SCHOOL
FOR TRAINING AND IMPROVEMENT OF JUDGES (ENFAM)**

On August 31, 2022, FDUC (Portugal) and ENFAM (Brazil) signed, through their top representatives, an Academic and Scientific Cooperation Agreement aimed at implementing joint and effective actions that would ensure the performance of academic activities related to teaching and research, by of their Research Centers and Institutes. The cooperation has involved the implementation of projects, research groups, international seminars, scientific publications, data sharing and exchange of experiences, among other products.

This book is another important product of the Scientific and Academic Cooperation Agreement between the two renowned higher education institutions, of the partnership between research groups, as well as of the collaboration of professors and researchers from the University of Salamanca.

ACKNOWLEDGEMENTS

This work is the result of research developed by renowned researchers on technological transformation and digital governance in the justice system, in their research centers. This connection between researchers has been important for the production of knowledge, as it allows knowledge to be developed from a global perspective.

In this sense, we would like to thank all the authors who contributed to this work based on their research, materialized in the chapters: Ana Carla Werneck, Inês Oliveira, Audrey Kramy Araruna Gonçalves, Irene González Pulido, David Soto, Irene Yáñez García-Bernalt, Fabrício Castagna Lunardi, Lorenzo-Mateo Bujosa Vadell, Federico Bueno de Mata, Pedro Miguel Alves Ribeiro Correia, Fernando Martín Diz, Ricardo Pedro, Francesco Contini, and Salomão Akhnaton Z. S. Elesbon.

We would also like to thank our institutions, which supported us in the research and production of this book: National School for the Training and Improvement of Magistrates – ENFAM (Brazil), University of Coimbra (Portugal) and University of Salamanca (Spain).

We would also like to thank the ENFAM team of librarians, who helped us standardize the text, especially the bibliographical references, in accordance with the Publisher's standards.

We would also like to give special thanks to the Press of the Legal Institute of the Faculty of Law of the University of Coimbra, which edited this work.

Finally, we would like to thank our readers, professors, researchers and students, who are the reason for this book.

Have a great read!

Brasília/Coimbra/Salamanca, March 2025.

Fabrício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell
Editors

Contents

Acknowledgements	9
-------------------------------	---

INTRODUCTION: AN OVERVIEW ON DIGITAL TRANSFORMATION AND GOVERNANCE IN THE JUDICIARY	15
Fabrício Castagna Lunardi, Pedro Miguel Alves Ribeiro Correia e Lorenzo-Mateo Bujosa Vadell	

PART I – THE VIRTUALIZATION OF JUSTICE: ANALYSIS OF DIGITAL JUSTICE FROM BRAZIL, ITALY AND SPAIN

CHAPTER 1

<i>The Virtualization of the Judicial Process in Brazil and the Performance of the National Council Of Justice in Digital Governance</i>	21
Ana Carla Werneck, Fabrício Castagna Lunardi e Pedro Miguel Alves Ribeiro Correia	
1. Introduction.....	22
2. Brazilian electronic process: the evolution	22
3. Effects of the virtualization on the reasonable duration of the judicial process	26
4. The PDPJ-BR as a result of the performance of the national council of justice in digital governance	30
5. Conclusions	34
References	34

CHAPTER 2

<i>Judicial Evolutions: From Paper to Digital Working Environment in the Italian Administration of Justice</i>	39
Francesco Contini	
1. Introduction	39
2. The Italian Justice System.....	40
3. The governance of e-government	41
4. E-justice in Italy: an overview	41
5. E-justice for civil proceedings	42
6. E-justice for criminal proceedings.....	44
7. Law and technology: entanglements and alignment	47
8. Concluding remarks: the impact on values and judicial governance	49
References	50

CHAPTER 3

Um Balanço das Políticas de Digitalização da Justiça em Espanha55

David Soto

1. Introdução	55
2. As políticas de digitalização da justiça em Espanha	56
2.1. O começo de tudo: a Lei 18/2011.....	57
2.2. Avançar afrontando os velhos e novos desafios: o Real Decreto-Lei 6/2023	58
2.3. Direitos digitais na administração de Justiça.....	59
2.4. Acesso digital à administração de Justiça	60
2.5. Tramitação eletrônica dos procedimentos judiciais	61
2.6. Atos processuais não presenciais.....	63
3. Resultados das políticas de digitalização em Espanha	65
3.1. A percepção das mudanças pela cidadania	65
3.2. A evolução da demora e da carga de trabalho judicial.....	66
3.3. A transformação das profissões jurídicas	69
3.4. Os desafios por diante	70
4. Conclusões	71
Referências	71

PART II – JUSTICE AND ONLINE DISPUTE RESOLUTION

CHAPTER 1

Justicia Digital y Virtual en los Medios Extrajudiciales de Resolución de Litigios77

Fernando Martín Diz

1. El entorno de la Justicia eficiente: desjudicializar, digitalizar y virtualizar.....	77
2. Automatización en la solución extrajudicial de litigios	80
3. Virtualización de las soluciones extrajudiciales de litigios	82
3.1. La figura del árbitro o mediador virtual y su posible responsabilidad civil	85
3.2. Automatización y funciones decisorias en la solución extrajudicial de litigios: complejidad y opciones	88
3.3. Virtualización de árbitros y mediadores.....	90
3.4. Hibridación como tercera vía para la aplicación de inteligencia artificial decisoria en solución extrajudicial de litigios	92
4. Bases del modelo tecnológico de solución extrajudicial de litigios.....	95
Referencias	97

CHAPTER 2

Consumer Litigation and Extrajudicial Resolution Platforms: a Case Study of the Civil Small Claims Courts in Espirito Santo (Brazil)101

Salomão Akhnaton Zoroastro Spencer Elesbon

1. Introduction.....	101
2. Procedural interest and extrajudicial platforms for resolving consumer conflicts.....	103
3. Profile of cases in Civil Small Claims Courts (JECS) of Espirito Santo.....	108
4. Major litigants and their participation in extrajudicial platforms	112
5. Feasibility of integrating extrajudicial platforms to the civil small claims Courts of Espirito Santo, Brazil.....	121
6. Conclusions	123
References	124

PART III – PEOPLE MANAGEMENT IN DIGITAL JUSTICE

CHAPTER 1

<i>Teleworking and the Right to Disconnect: the Brazilian Experience</i>	131
Audrey Kramy Araruna Gonçalves	
1. Introduction.....	131
2. Teleworking.....	132
2.1. Regulation and expansion.....	132
2.2. Teleworking in the Brazilian Judiciary	135
2.3. Impact of Digital Transformations on Management Models.....	137
3. Right to disconnect.....	139
4. Case Study of a Brazilian State Court of Justice.....	141
5. Conclusions	143
References	144

PART IV – DATA MANAGEMENT: JUDICIAL TRANSPARENCY, LITIGANCE AND PROTECTION OF PERSONAL DATA

CHAPTER 1

<i>Algoritmos Digitais: Uso Público, Transparência e Litigância</i>	149
Ricardo Pedro	
1. Introdução	149
2. Uso Público de Algoritmos	150
3. (In)Transparência Algorítmica	152
4. Transparência no uso Público de Algoritmos.....	154
4.1. Introdução	154
4.2. Acesso ao Código Fonte	155
5. Litigância.....	157
5.1. Introdução	157
5.2. Caso “SyRI”	157
5.3. Caso “Fundação Civio”	158
5.4. Caso “COMPAS”	158
5.5. Alguns problemas jurídicos.....	159
6. Conclusões.....	163
Referências	164

CHAPTER 2

<i>A Proteção de Dados Pessoais e o Sistema Judicial Português: o que está por fazer em 2023? ..</i>	169
Inês Oliveira	
1. Introdução	170
2. O regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial.....	170
3. O que está por fazer?	172
3.1. A alteração da Lei n.º 34/2009	172
3.2. Os tipos de dados judiciais: a fronteira entre dados processuais e dados administrativos	173
3.3. A publicidade versus publicitação do processo	174
3.4. A designação do encarregado de proteção de dados nos tribunais	175
3.5. A formação aos operadores judiciários	175

4. Conclusão	175
Referências	176

PART V – NEW TECHNOLOGIES IN THE ADMINISTRATION OF JUSTICE: BLOCKCHAIN, ARTIFICIAL INTELLIGENCE AND CRIMINAL INVESTIGATION

CHAPTER 1

<i>Evidentiary Aspects of the Blockchain: Analysis of the Legal Reality in Europe and Spain.....</i>	179
Federico Bueno de Mata	
1. Genesis of a revolution at the evidentiary level.....	179
2. A legal regulatory framework for the use of blockchain technology at the evidentiary level	181
3. Procedural treatment of the blockchain.....	184
4. Final reflections: looking at the Web3	187
References	188

CHAPTER 2

<i>El Uso de la Inteligencia Artificial en la Comisión e Investigación del Delito de Child Grooming</i>	191
Irene Yáñez García-Bernalt	
1. Introducción: la irrupción de la inteligencia artificial en la esfera jurídica	192
2. El auge de la ciberdelincuencia sexual.....	192
2.1. La vulnerabilidad de los menores de edad en el mundo online	194
2.2. Aproximación al fenómeno <i>child grooming</i>	195
3. Inteligencia artificial (ia) y corrupción de menores.....	197
3.1. El uso de la IA en la perpetración del delito de child grooming	197
3.2. La IA como herramienta en la investigación de delitos de corrupción de menores	198
4. Conclusiones.....	201
Referencias	202

CHAPTER 3

<i>Órdenes Europeas para Reforzar la Cooperación Policial y Judicial en Casos de Delincuencia Sexual Transfronteriza.....</i>	205
Irene González Pulido	
1. Delincuencia sexual y la expansión de internet: ¿ante qué fenómeno se enfrenta la comunidad internacional?	206
2. Herramientas legales y policiales que se han implementado en las últimas décadas para hacer frente a este fenómeno	208
3. Órdenes europeas que marcan el devenir de la cooperación policial y judicial internacional.....	215
4. Reflexiones finales: para mejorar la respuesta y represión delictiva de estas tipologías delictivas.....	219
Referencias	222

CHAPTER 2 – EL USO DE LA INTELIGENCIA ARTIFICIAL EN LA COMISIÓN E INVESTIGACIÓN DEL DELITO DE *CHILD GROOMING*

(DOI: 10.47907/DigitalTransformationAndGovernance/10)

Irene Yáñez García-Bernalt¹

“¿Por qué esta magnífica tecnología científica que ahorra trabajo y nos hace la vida más fácil, nos aporta tan poca felicidad? La respuesta es esta: simplemente porque aún no hemos aprendido a usarla contino”

(Albert Einstein, 1879-1955)

Sumario: 1. Introducción: la irrupción de la Inteligencia Artificial en la esfera jurídica. 2. El auge de la ciberdelincuencia sexual. 2.1. La vulnerabilidad de los menores en el mundo online. 2.2. Aproximación al fenómeno *child grooming*. 3. Inteligencia Artificial (IA) y corrupción de menores. 3.1. El uso de la IA en la perpetración del delito de *child grooming*. 3.2. La IA como herramienta en la investigación de delitos de corrupción de menores. 3.2.1. Reflexiones sobre la implementación de la IA en la fase de instrucción. 3.2.2. Policía predictiva y *child grooming*. 4 Conclusiones. 5. Referencias.

Resumen: La inminente implementación de las tecnologías disruptivas y su cada vez mayor alcance en todas las esferas de la sociedad ha generado incontables beneficios, a la par que se han puesto de manifiesto importantes riesgos en cuanto a su uso. La Inteligencia Artificial se erige como un recurso eficaz para la comisión de ilícitos penales viralizándose fenómenos como el *face swap* o *deepfake*, convirtiéndose en un mecanismo de engaño que encuentra su encaje en el delito de corrupción de menores o *child grooming*. Si bien el uso de la misma se alza, a su vez, como un excelente mecanismo para la investigación de dichas conductas.

Palabras Clave: menores, víctima, Inteligencia Artificial, tecnología.

Abstract: The imminent implementation of disruptive technologies and their increasing reach in all spheres of society has generated countless benefits, while significant risks have been revealed regarding their use. Artificial Intelligence emerges as an effective resource for the commission of criminal offenses, making phenomena such as face swap or deepfake go viral, becoming a deception mechanism that finds its place in the crime of corruption of minors or child grooming. Although its use stands, in turn, as an excellent mechanism for the investigation of said behaviors.

Keywords: minors, victim, Artificial Intelligence, technology.

¹ Personal Investigador en Formación en el área de Derecho Procesal (Universidad de Salamanca). E-mail: ireneygb@usal.es ORCID: <https://orcid.org/0000-0001-8859-6029>. Trabajo realizado en el marco de la convocatoria de contratos predoctorales (Programa Propio III) USAL 2020, cofinanciada por el Banco Santander.

1. Introducción: la irrupción de la inteligencia artificial en la esfera jurídica

La llegada de las nuevas tecnologías a la vida del ser humano ha traído como principal consecuencia una mejora en las condiciones de desarrollo tanto a nivel individual como colectivo. Internet ha permitido generar un grado de hiperconectividad altamente elevado estrechando lazos y comunicaciones a cientos de miles de kilómetros. Sin embargo, nuestra privacidad, seguridad e incluso esas mencionadas interacciones sociales se han puesto en riesgo. La irrupción de otras tecnologías como la Inteligencia Artificial (en adelante, IA) y la automatización han venido a transformar todas las esferas de la sociedad. Estamos ante una revolución 4.0 basada en un proyecto de estrategias de alta tecnología (Barona Vilar, 2021) que brinda mejoras en el mercado. No obstante, en esta era digital, los derechos y libertades que el Estado debe amparar no pueden huir a las terminaciones de dicho mercado, del poder económico, debiendo limitarse mediante una política de índole humanista (Dolz Lago, 2022)

Si nos alejamos del foco económico, en el que esta nueva tecnología ha tenido un importante impacto, y ponemos la atención en el mundo jurídico, podemos afirmar, sin lugar a duda, que la IA y el Derecho son dos esferas en constante fusión. Desde el punto de vista de la eficacia y la eficiencia en el mundo del Derecho, concebimos la IA como una importante herramienta para la automatización de determinadas tareas, como puede ser la revisión de documentos. Pero es que, además, puede ser empleada para mejorar la toma de decisiones mediante un exhaustivo análisis de datos y predicciones basadas en ciertos patrones. (Martín Diz, 2021). Sin embargo, cuando analizamos la otra cara de la moneda, somos conscientes de cómo el poder y la versatilidad de la IA ofrece las consecuencias negativas de su uso, entre las que se incluye la comisión de ilícitos penales. Aunque la IA puede ser empleada para la prevención y combate de la delincuencia, también resulta desafiante para la seguridad. Hablamos de una ciberdelincuencia mucho más avanzada, dado que permite el desarrollo de malwares mucho más sofisticados que los ofrecidos hasta ahora, siendo así más sencilla la identificación de las vulnerabilidades de los sistemas informáticos y la posibilidad de eludir las barreras de seguridad. De igual modo la creación de falso contenido es mucho más real y convincente a través de la IA, hablamos aquí de la generación y de imágenes y vídeos manipulados conocido como *DeepFake*. Multitud de aplicaciones móviles permiten la manipulación de fotografías, lo que ha supuesto un incremento de la aparición de imágenes y vídeos de carácter pornográfico con los rostros de menores de edad (Fernández Senac, 2023). En definitiva nos encontramos aquí con que la prevención, investigación y comisión de tales delitos, empleando la IA, plantea una serie de desafíos tanto legales como éticos, siendo las autoridades las encargadas de equilibrar los beneficios y perjuicios provocados por esta tecnología, especialmente cuando se trata, como se abordará en las siguientes líneas, de delitos contra colectivos especialmente vulnerables como son los menores de edad.

2. El auge de la ciberdelincuencia sexual

Los delitos sexuales en línea, delitos cibernéticos sexuales o ciberdelitos sexuales constituyen actividades delictivas que involucran el uso de las TICs, Internet y otros dispositivos informáticos

para cometer actos de carácter sexual ilegales, cuyo alcance global plantea una serie de desafíos en la aplicación de la ley y la protección de las víctimas. En el año 2021, siguiendo el Informe sobre la Cibercriminalidad en España elaborado por el Ministerio de Interior, se registraron un total de 1198 victimizaciones por delitos sexuales² de las cuales el rango de edad más afectados son los menores (0-17 años), constituyendo de ese total señalado, 1053 víctimas. Es decir, que los menores de edad víctimas de esta tipología delictiva constituye el 36%. El incremento de este tipo de conductas muestra cifras desoladoras en relación con los menores de edad, pues el uso masivo de las tecnologías aumenta el riesgo de exposición a formas de interacción sexual (Tamarit Sumalla, 2018)

El auge de los ciberdelitos sexuales se debe así, en gran parte, a la creciente y constante interconexión digital y a la intensificación producida respecto de la actividad en línea. Si esbozamos más detalladamente el trasfondo de las razones mencionadas, nos encontramos con que la producción de las mismas se debe, en primer lugar, la facilidad de acceso a las plataformas. La cantidad de material de carácter sexual disponible en redes ha crecido significativamente en los últimos años en forma de *banners* y anuncios que aparecen sin que lo deseemos. Ello puede conducir a la normalización de estos comportamientos y aumentar el deseo y tentación de participar en ellos. En segundo lugar, las redes sociales y las aplicaciones de mensajería instantánea como *Instagram*, *Twitter* –ahora “X”, *TikTok*, *WhatsApp* o *Telegram*, cuyo uso se ha visto incrementado desde la pandemia del COVID-19 (Méndez y Pérez Fernández, 2020), se erigen como canales de comunicación donde los agresores pueden comunicarse fácilmente con sus potenciales víctimas –especialmente con menores de edad– y conseguir manipularlos o coaccionarlos para participar en actos sexuales a través del engaño. En tercer lugar y enlazado con el perfil del delincuente, se encuentra el anonimato que ofrece Internet, pues existen cientos de vías, muchas de ellas sencillas, para ocultar la identidad y aumentar así la sensación de impunidad. En cuarto lugar podemos hablar de la denominada “ingeniería social”. Se trata de una técnica de manipulación psicológica que involucra el engaño del personal autorizado en un sistema informático y obtener así información sensible (López Grande y Salvador Guadrón, 2015). Por lo tanto, resulta útil el empleo de estas técnicas en la comisión de ciberdelitos sexuales para manipular y explotar a la víctima. La finalidad es hacer uso de esa confianza generada con la persona objetivo de la conducta para obtener material sexualmente explícito o para llevar a cabo otro tipo de abusos de esta índole.

A esas cuatro explicaciones debemos añadir, además, la falta de conciencia y educación tanto digital como sexual. Ello, en tanto en cuanto, la mayoría de los jóvenes no son completamente conscientes de los peligros de interacción con extraño en línea o de compartir contenido de carácter sensible de forma no consensuada. Asimismo, se han de tener en cuenta los desafíos técnicos. Los delincuentes sexuales online utilizan técnicas, en muchas ocasiones, demasiado

² Se excluyen aquí las agresiones sexuales con o sin penetración y los abusos sexuales derogados por la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

sofisticadas como la manipulación de imágenes –a través de la IA– o de suplantación de la identidad para cometer el engaño y, por ende, el ilícito penal.

2.1. La vulnerabilidad de los menores de edad en el mundo online

La plataforma *We are social* en la elaboración de su Informe Digital 2022 muestra una tendencia al alza del uso de plataformas digitales que ya supera los datos recabados antes de la pandemia del COVID-19. El número de usuarios en las redes sociales equivale a una cifra superior al 58% de la población mundial. *YouTube*, *WhatsApp* y *TikTok* son las plataformas con mayor número de usuarios registrados. En España 2.4 millones de usuarios son menores de entre 13 y 17 años, cifra que merece especial atención en tanto en cuanto varios de sus bienes jurídicos protegidos pueden verse afectados negativamente por el uso de dichas plataformas (Ayllón García, 2022), especialmente cuando se trata de la indemnidad y libertad sexual. Resulta ciertamente llamativa esta cifra cuando el legislador establece límites de edad para acceder a las redes sociales. Si bien es cierto que en la actualidad somos testigos de la facilidad existente para poder prestar ese consentimiento, debido a la falta de mecanismos para acreditar la autenticidad y verificación de la edad (Guardiola Salmerón, 2016).

Tanto a nivel nacional como internacional³, el legislador se ha mostrado especialmente sensible a la hora de reforzar la protección de la indemnidad sexual ante este tipo de conductas cuando se trata de víctimas especialmente vulnerables (Rodríguez Tirado, 2018). La condición de vulnerabilidad de una víctima reside en las circunstancias personales, sociales, económicas y culturales que la rodean⁴, y se manifiesta en la debilidad a la hora de comprender y asimilar cierto tipo de información, la forma de hacer frente y protegerse ante determinados tipos de conductas y también dicha vulnerabilidad se traduce en una falta o disminución de la aquiescencia para realizar, por ejemplo, conductas de carácter sexual. Desde la óptica del mundo virtual la vulnerabilidad de los menores se aprecia en la concurrencia de diversos factores. En primer lugar, la exposición a contenido inapropiado tales como vídeos y fotografías con lenguaje violento, material extremista o contenido de carácter pornográfico, lo cual hace que pueda generar importantes perjuicios en su desarrollo emocional y psicológico. En segundo lugar, la falta de privacidad o, más bien, la falta de consciencia sobre los riesgos vinculados a la privacidad en línea. Los menores de edad son más propensos a compartir información personal –su ubicación en tiempo real o datos de contacto– de manera imprudente, de modo que esto puede ser aprovechado y explotado por ciberdelincuentes. Y, en tercer lugar, estaría la falta de discernimiento a la hora de

³ Véase en este sentido la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

⁴ Seguimos la definición aportada por las 100 Reglas de Brasilia sobre acceso a la justicia de las personas en condición de vulnerabilidad de la XIV Cumbre Judicial Iberoamericana (2008).

discriminar determinados tipos de información siendo más compleja su distinción entre datos de carácter confiable y *fake news*, siendo así más propensos a creer en falsas teorías.

La combinación de todos estos factores conduce a la conversión de los menores en potenciales víctimas de espeluznantes conductas que se pueden llevar a cabo fácilmente a través de dispositivos informáticos. Evidentemente, ello presenta importantes consecuencias tanto a nivel penal como procesal. Desde el punto de vista del derecho penal sustantivo, el legislador, consciente de la vulnerabilidad inherente a los menores de edad, ha optado por recurrir a técnicas variadas para garantizar una adecuada tutela penal de los menores (Blanco Cordero, 2023). Así encontramos un capítulo de nuestro CP dedicado exclusivamente a las agresiones sexuales a menores de 16 años o también prevé una agravación de la pena cuando se utilice también a menores de 16 años en espectáculos de carácter pornográfico. Desde la perspectiva del derecho procesal, la vulnerabilidad va a ser tenida en consideración en el momento en que el menor ostenta la posición de víctima del delito, lo cual va a generar la activación de una serie de alarmas y protocolos especiales en las diversas actuaciones como puede ser, a modo de ejemplo, la toma de declaración y su consideración como prueba preconstituida⁵.

En definitiva, nos encontramos con un colectivo que, si bien está integrado por los que denominaríamos *nativos digitales*, lo cierto es que no deja de ser una generación especialmente sensible al uso y la evolución de las nuevas tecnologías (Abadías Selma, 2022), así como al contenido que circula de manera libre y sin filtro alguno a lo que se debe añadir, incluso, la exposición temprana sin su consentimiento, por parte de sus padres a través del fenómeno *sharenting*, viéndose así atacada su intimidad personal y su honor.

2.2. Aproximación al fenómeno *child grooming*

El uso cada vez más generalizado de las redes sociales y las plataformas digitales por parte de los menores de edad, sumado a su vulnerabilidad conducen, en numerosas ocasiones, a la conversión de los mismos en potenciales víctimas de ciberdelitos, la mayoría, de carácter sexual (Gutiérrez Azanza, 2020). El Informe sobre Delitos contra la Libertad e Indemnidad Sexual de 2021 elaborado por el Ministerio del Interior muestra unas cifras desoladoras en materia de ciberdelincuencia sexual. Ese año hubo un total de 1344 menores víctimas de delitos sexuales cometidos a través de medios tecnológicos, esto implica que 8 de cada 10 casos conocidos tienen como víctimas a menores. El delito de corrupción de menores es el segundo que más victimizaciones registra en el señalado año –un total de 217–, estando por encima el contacto a través de la tecnología con un menor de 16 años –un total de 440–.

Precisamente el delito de corrupción de menores, conocido bajo el anglicismo de *child grooming*, ha sido protagonista de un importante auge en los últimos años. Esta conducta pasa a ostentar la consideración como de delito en el art. 183 bis de nuestro CP a través de la reforma

⁵ Modificación introducida en el art. 449 ter LECrim con la entrada en vigor de la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia.

operada por la LO 5/2010, de 22 de junio, adelantándose a la ya mencionada Directiva 2011/93/UE. Posteriormente, con la LO 1/2015, de 30 de marzo, la ubicación del mencionado tipo penal cambia y pasa a quedar recogido en el art. 183 ter CP. Actualmente, tras la reforma operada por la LO 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, su ubicación se encuentra en el art. 183 CP. También se ha de hacer mención a los esfuerzos realizados a través de la LO 8/2021, de 4 de junio, de protección a la infancia y la adolescencia frente a la violencia (LOPIVI, en adelante) a través de la cual se introduce cambios en el cómputo del tiempo de prescripción de los delitos contra la indemnidad sexual. Así, en estos casos, cuando la víctima sea menor de edad, el tiempo empezará a contar desde que esta cumpla los 35 años, salvo que fallezca antes, de modo que comenzará a contar desde la fecha de fallecimiento.

Vista la normativa que trata de proteger al menor frente al embaucamiento y corrupción sexual, la siguiente tarea es la de aproximarnos hacia el contenido de este tipo de conducta. El término *child grooming* hace alusión a las acciones realizadas de manera deliberada con el fin de entablar una relación y consolidar un control emocional sobre el menor de edad preparando así el terreno para la agresión sexual⁶. Esas acciones, para que encajen en el tipo penal señalado, en primer lugar, deben ser realizadas a través de Internet, teléfono o cualquier dispositivo tecnológico. En segundo lugar, la víctima debe ser menor de 16 años. En tercer lugar y último lugar, la propuesta se debe acompañar siempre de actos materiales encaminados al acercamiento con el menor. Así pues, este delito se caracteriza porque puede darse en diferentes contextos, ya sea en redes sociales, chats en línea, juegos online y otras plataformas digitales e incluso en el metaverso. El delito se caracteriza así por emplear técnicas de control y manipulación, sobre sujetos especialmente vulnerables –como son los niños y adolescentes–, en entornos sociales y digitales diversos con la finalidad de ganar la confianza de sus víctimas ya sea ofreciendo atención, afecto o incluso falsas promesas de fama o éxito y así poder allanar el terreno para la explotación o exposición prohibida del menor (Abadías Selma, 2020). Así realmente el delito se configura en torno al peligro que supone para la libertad e indemnidad sexual del menor⁷. En cuanto al papel del infractor, denominado *groomer*, se trata de un adulto que busca agredir sexualmente a menores haciendo uso de las nuevas tecnologías. Para poder llevar a cabo esta conducta, crean perfiles falsos en sus respectivas redes sociales y plataformas online para entablar prolongadas conversaciones y ganar contenido sexual explícito del menor víctima. Una vez logrado este propósito, comienzan el chantaje y las amenazas al menor sobre la publicación de tales fotos si no entrega más o se niega a un encuentro físico⁸. Téngase en cuenta que la negativa del menor al envío de más material o al posible encuentro cara a cara, puede llevar al autor al envío de tales fotografías incurriendo así en un delito de sextorsión, dado que el material es enviado sin el consentimiento de la víctima (Magro Servet, 2023). En definitiva, el *child grooming*

⁶ Vid. STS 97/2015, de 24 de febrero.

⁷ Ídem.

⁸ Vid. STS 174/2017, de 21 de marzo.

supone, en parte, un cierto abuso de poder que termina generando un aislamiento de la víctima alejándola de su círculo más cercano.

3. Inteligencia artificial (ia) y corrupción de menores

3.1. El uso de la IA en la perpetración del delito de child grooming

Como se ha explicado en las líneas anteriores, el delito de *child grooming* se caracteriza por ser un delito de carácter informático y sexual, es decir, un ciberdelito sexual. Como toda conducta de estas características, el paso del tiempo y la creación de nuevas formas de comunicación así como el avance de las tecnologías, hace que este delito también se adapte a los nuevos tiempos.

El uso de la IA para automatizar las ya mencionadas herramientas de ingeniería social constituye una tendencia dentro del cibercrimen (Martínez Vázquez, 2020). Podemos afirmar, sin lugar a duda, que el uso de la IA para delinquir constituye una creciente preocupación en el campo de la ciberdelincuencia. A pesar de las beneficiosas aplicaciones, la IA también es empleada por los criminales para llevar a cabo actividades ilícitas. Precisamente, el incremento en la comisión del ilícito penal del *child grooming* se encuentra vinculado, además de al uso masivo de las redes sociales, a la evolución en las formas de perpetración del delito, siendo la IA una herramienta idónea en este tipo penal.

El uso de la IA en la comisión del delito de *child grooming* puede tener diversas manifestaciones. En primer lugar, puede ser empleada para la identificación de víctimas potenciales. Esto es, el empleo de algoritmos creados a través de la IA para identificar a posibles víctimas en línea. Estos algoritmos pueden analizar el comportamiento de los menores de edad en el mundo online, sus interacciones en redes sociales y su actividad, lo cual serviría para dar con aquellos que muestran mayor vulnerabilidad. En segundo lugar, la IA también puede ser utilizada para persuadir y manipular a los menores. Nos referimos aquí al uso de *chatbots*, es decir de conversaciones automáticas, o programas que simulan ser personas reales para generar así una relación de confianza con el niño o adolescente y generar una manipulación emocional. En tercer lugar, encontramos la generación de contenido inapropiado. A través de la IA es posible crear contenido sexualmente explícito, imágenes o vídeos, que involucre a menores de edad.

Uno de los usos de la IA que encuentra su encaje en este tipo de delito es el del *DeepFake*. Esta técnica, inicialmente utilizada para la manipulación de imágenes y vídeos con carácter lúdico y recreativo, puede alcanzar importantes niveles de preocupación en tanto en cuanto estamos ante una manipulación de rasgos biométricos, ya que están relacionados con la identificación de una única persona. Los rasgos biométricos incluyen huellas dactilares, el reconocimiento facial de la voz o el escaneo, por ejemplo, del iris. Estamos pues, ante una auténtica categoría de datos personales que son obtenidos a través de un tratamiento técnico muy concreto y que son relativos a las características físicas de una persona (Etxebarria Guridi, 2022). Existen múltiples usos del *DeepFake* en relación con el delito de *child grooming* y en la afectación de los rasgos biométricos. En primer lugar, los ciberdelincuentes pueden hacer uso de los *DeepFakes* para elaborar material que involucre a menores de edad, aunque las personas representadas en dicho

material sean adultos. En segundo lugar, esta herramienta también es útil para llevar a cabo una suplantación de la identidad. Pueden crear *DeepFakes* haciéndose pasar por menores para generar esa confianza con la potencial víctima y así obtener el contenido sexual de esta. Asimismo, también este mecanismo de IA es viable para la extorsionar o sextorsionar y amenazar a las víctimas.

Así pues, el *DeepFake* y también el *Face Swap* (herramienta creada a través de IA que también permite la manipulación de imagen, vídeo y sonido), constituyen herramientas eficaces en el *modus operandi* inherente al delito de *child grooming*, a la hora de generar contenido falso que conferirá, bajo el anonimato, una mayor facilidad para entablar la relación de confianza con la víctima menor de edad y obtener así el material sexual para su posterior distribución en la red así como para llevar a cabo una sextorsión.

3.2. La IA como herramienta en la investigación de delitos de corrupción de menores

3.2.1. Reflexiones sobre la implementación de la IA en la fase de instrucción

Vista la parte negativa del uso de la IA en relación con la posibilidad de llevar a cabo conductas penalmente reprochables, lo cierto es que el prisma de esta novísima herramienta también ofrece ciertas ventajas dentro del proceso penal. Ya somos testigos de las primeras mejoras implementadas en la administración de justicia gracias al procesamiento de datos mediante algoritmos inteligentes, o su uso para la valoración del riesgo, así como su empleo en materia probatoria para contrastar datos de manera objetiva (Martín Diz, 2022).

Antes de la concepción de la IA como una posible vía para la investigación en el proceso penal, en su momento, la LO 13/2015, de 5 de octubre, incorpora a nuestra la LECrim las denominadas diligencias de investigación tecnológicas, las cuales permiten el acceso a las fuentes de prueba digital. No se trata, ni mucho menos, de una cuestión baladí, pues la norma pasa a dar respuesta legal a una realidad de las potencialidades prácticamente ilimitadas de las nuevas tecnológicas en la investigación de delitos (Rodríguez Lainz, 2018). Estas se introducen en nuestro ordenamiento jurídico con suma cautela ponderando, siempre, la injerencia que producen en los derechos fundamentales (Ortego Pérez, 2022) y bajo el prisma de una serie de principios rectores: especialidad, idoneidad, excepcionalidad y necesidad y, por último, el principio de proporcionalidad.

Ahora bien, como era de esperar, los avances tecnológicos producidos en la manera de cometer ilícitos penales también llevan aparejados la implementación de nuevas formas de investigación criminal. Por ello la aplicación de la IA ha supuesto una auténtica revolución a la hora de facilitar el esclarecimiento de los hechos. Este importante progreso o avance no se refiere únicamente a la aparición de estos medios, sino a la eficacia que pueden presentar en la fase de instrucción (Muñoz Rodríguez, 2020) pudiendo adquirir la consideración de una nueva diligencia de investigación. La aplicación de la IA en el proceso penal constituye, pues, una realidad. Sobre sus posibilidades misma en el art. 516 del Anteproyecto de la Ley de Enjuiciamiento Criminal de 2020, donde se recoge la posibilidad de que el juez autorice, a instancia del MF, la utilización de sistemas automatizados o inteligentes en el tratamiento de datos para interrelacionar la información sobre el sujeto investigado.

Evidentemente, al igual que ocurre en su momento con las diligencias de investigación tecnológicas, la incorporación de los sistemas inteligentes al proceso penal debe velar por el equilibrio entre los derechos y garantías que conforman la fase de investigación (San Miguel Caso, 2022). el empleo de esta tecnológica se encuentra supeditada a la concurrencia de una serie de requisitos, pues no deja de producirse una injerencia en datos que tienen la consideración de sensibles. Sobre esas circunstancias condicionantes, en primer lugar, se requiere que existan indicios basados en datos objetivos sobre la participación del investigado en los hechos de la investigación. Este requisito se vincula directamente con el principio de proporcionalidad, en virtud del cual el juez valorará y ponderará el que el sacrificio de los derechos e intereses de los afectados no sea superior al beneficio que de su adopción resulte para el interés público. Para la ponderación se tendrá en cuenta, entre otros aspectos, la intensidad de los indicios existentes constituyendo este un importante parámetro que permitirá calibrar el grado de desarrollo de la conducta delictiva y la participación del investigado. De este modo se obtendrá un análisis más meditado sobre el nivel de injerencia en el derecho fundamental de que se trate⁹.

En segundo lugar, se hace alusión a la necesaria práctica de esta diligencia teniendo en cuenta la naturaleza y las características del hecho. El uso de estos sistemas se considera como algo excepcional y no rutinario, de modo que la justificación de su adopción reside en que no existe otra medida lícita eficaz para la averiguación del delito¹⁰. Por último, el art. 516 del Anteproyecto LECrim 2020 alude a la necesidad de que el hecho investigado sea constitutivo de un delito castigado con una pena igual o superior a los tres años de prisión. Requisito que se contempla en otras diligencias de investigación tecnológicas como la interceptación de las comunicaciones telefónicas y telemáticas (Art. 588 ter LECrim).

3.2.2. Policía predictiva y child grooming

La lucha contra las nuevas formas de criminalidad basadas en la tecnología ha traído consigo, como ya veníamos apuntado, la necesaria instauración de herramientas de investigación basadas en la acumulación, tratamiento y análisis de datos. En relación con la investigación del delito de *child grooming*, consideramos que una de las herramientas basadas en la IA que presentaría una mayor eficacia en esta fase de esclarecimiento de los hechos es, precisamente, la policía predictiva. Esta herramienta se basa en el uso de una importante cantidad de datos que son analizados para estimar, a través de algoritmos, un valor que es desconocido y sus resultados deberían servir para gestionar de manera más eficaz los recursos policiales (Borges Blázquez, 2022). Por lo tanto, se trata de una estrategia de aplicación de análisis de datos y tecnología avanzada basada en el uso de datos históricos en tiempo real y en modelos de aprendizaje automáticos para

⁹ Véase la Circular 1/2019, de 6 de marzo, del Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.

¹⁰ Sobre esta cuestión se pronuncia nuestro TS en relación con la interceptación de las comunicaciones telefónicas. Véase la STS 279/2017, de 19 de abril.

poder anticipar los patrones delictivos. Los aspectos clave de la policía predictiva se centran, en primer lugar, en la recopilación de datos (pensamos aquí en la inclusión, por ejemplo, de informes de incidentes previos, registros criminales, datos demográficos o ubicaciones geográficas). En segundo lugar, estaría el análisis de datos a través de algoritmos de aprendizaje automático y análisis estadísticos para la correcta identificación de patrones y tendencias. En tercer lugar, la predicción y evaluación de los riesgos, con base en el análisis previamente realizado, la policía predictiva generaría predicciones sobre las áreas geográficas o momentos en los que es más probable que ocurra el delito. En cuarto lugar, esta herramienta como ya mencionábamos puede ser eficaz para mejorar el despliegue de recursos enviando, por ejemplo, patrullas en los momentos de mayores riesgos. Y, por último, puede ser empleada para prevenir el crimen a través de una mayor visibilidad de las áreas de riesgo. En España ya se ha desarrollado alguna herramienta de policía predictiva, como es Veripol, que analiza y estima la posibilidad de que las denuncias por robo con violencia o intimidación sean falsas (López Pérez, 2022). Otra de esas herramientas es VioGén, la cual está vinculada a la creación y valoración de un protocolo sobre el riesgo de reincidencia en materia de violencia de género (González-Álvarez. Santos-Hermoso. Camacho-Collados, 2020).

En relación con el delito de *child grooming*, se trata de una conducta que presenta importantes dificultades en materia de prevención e investigación, lo cual implica un importante estudio sobre los factores de riesgo, la relación de los menores con el uso de internet y el análisis de estudios cualitativos sobre los adultos abusadores (De Santiesteban. Gámez Guadix, 2017). Por ello resulta interesante el posible uso de una de las herramientas de la policía predictiva: CATT (*Chat Analysis Triage Tool*). Se trata de un algoritmo creado por el Instituto Politécnico de la Universidad de Purdue (Indiana) que se erige como una herramienta de investigación basada en mecanismos de procesamiento del lenguaje natural, analizando y comprando chats y conversaciones online entre menores y depredadores sexuales en línea impulsados por el contacto (Seigfried-Spellar, *et al.*, 2019). A través de un análisis sobre las diferencias basadas en el idioma y factores como la autorrevelación –táctica en la que el depredador intenta generar confianza compartiendo una historia personal de carácter negativo, como puede ser, por ejemplo, el haber sufrido abusos en la infancia-, se puede crear una evaluación de riesgos y una probabilidad de que ese sujeto intente mantener un contacto físico con la víctima. Así los miembros de las FCSE pueden comenzar a priorizar aquellos casos en qué quieren destinar sus recursos de una manera más rápida. En España, desde la Secretaría de Estado y Seguridad ya se ha impulsado un proyecto de policía predictiva para los casos de *child grooming* basado el algoritmo antes mencionado. A lo que se debe sumar el uso de la niña virtual *Sweetie*, la cual conversa en plataformas de chat con posibles pederastas y depredadores sexuales online. (Borges Blázquez, 2022).

En definitiva el uso de la policía predictiva en la lucha contra la explotación sexual de menores en línea y en la investigación de delito de *child grooming* se alza como una herramienta, cuanto menos, útil, para la identificación de los sospechosos y el perfil de las víctimas. A través de un análisis de patrones de comportamientos en línea las FCSE pueden detectar la presencia de un posible depredador sexual. Para ello también será necesaria la inclusión de herramientas

de monitoreo de análisis del lenguaje que analicen las interacciones en redes sociales o detecten la realización de actividades ilegales en foros relacionados con la pedofilia. Precisamente, en relación con ese monitoreo, cabría la adopción de herramientas de monitoreo en redes peer-to-peer (P2P) para el rastreo de movimientos en los que se comparta material pornográfico infantil.

4. Conclusiones

A modo de conclusión, tras las explicaciones vertidas en las páginas que nos preceden llegamos a la reflexión de que nos encontramos en un momento oscuro, un momento en que el auge de la ciberdelincuencia sexual es una realidad que se encuentra al alza en esta era digital en la que estamos inmersos. El uso masivo de las redes sociales y la constante exposición de menores en Internet contribuyen a la comisión de estas conductas. No obstante, la tecnología supone un desafío para la aplicación de la ley y, lejos de paralizarse, la aparición de nuevas herramientas creadas a través de la IA supone una cierta ventaja y eficacia en la comisión de este tipo de conductas. Más allá de una regulación legal de carácter preventivo, aquí también entra en juego la colaboración de autoridades y empresas tecnológicas para tomar medidas en aras de combatir el uso de la IA en ciberdelitos. Esto incluye el desarrollo de herramientas de detección de *DeepFakes*, el uso de medidas de seguridad más sólidas, la colaboración con asociaciones y organizaciones dedicadas a la lucha contra las agresiones sexuales infantiles en línea y una mayor colaboración por parte de las plataformas digitales y redes sociales, véase en este sentido la negativa de algunas de ellas para proporcionar datos referidos, por ejemplo, a la IP de un dispositivo.

El legislador ha de ser cauto, pero también previsor, debiendo renovar la legislación existente en materia de detección e investigación de estas conductas cuando el fenómeno ya se ha producido. Previsor, por el creciente y constante aumento de las deplorables conductas que hemos venido señalando. Y cauto porque la regulación legal de diligencias de investigación basadas en la IA va a suponer una importante injerencia de determinados derechos fundamentales, al igual que ocurre con la incorporación a nuestro ordenamiento jurídico, en 2015, de las diligencias de investigación tecnológicas. No obstante, nada impide que, mediante la concienciación y la ponderación de los derechos afectados y el resultado que se pretende lograr el uso de la IA, estas medidas puedan ser implementadas y reguladas legalmente en nuestra LECrim.

Por último, es importante incidir en que la aplicación de la policía predictiva en la lucha contra el delito del *child grooming* debe llevarse a cabo haciendo una ponderación entre la ética y el deber de investigación, debiendo velar por la protección de la privacidad y no generando un perjuicio en los derechos fundamentales que sea mayor que el beneficio que podamos obtener de su uso en la investigación. Asimismo, resultará fundamental además la cooperación jurídica internacional y la colaboración entre agencias para abordar de manera eficaz este problema, dado que este tipo de conductas trascienden toda frontera física.

Referencias

- ABADÍAS SELMA, Alfredo, «El peligro de sobreexposición de los menores a internet frente al *child grooming* en tiempos del covid-19», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, 144 (Ejemplar dedicado a: Delitos en tiempos de emergencia sanitaria) (2020) 1-31.
- «Los menores como colectivo vulnerable en la era de la “cultura touch”», in Daniel FERNÁNDEZ BERMEJO; Enrique SANZ DELGADO, ed., *Tratado de delincuencia cibernética*, Aranzadi: Thomson Reuters, 2021, 75-118.
- AYLLÓN GARCÍA, Jesús Daniel, «Consentimiento de los menores de edad en las redes sociales: especial referencia a TikTok», *Actualidad Jurídica Iberoamericana* [em linha], 16 (Fev. 2022) 580-609, [consult. 18 Maio 2024]. Disponível em: <<https://www.revista-aji.com/wp-content/uploads/2022/04/24.-Jesús-Daniel-Aillón-580-609.pdf>>.
- BARONA VILAR, Silvia, *Algoritmización del derecho y de la justicia: de la inteligencia artificial a la smart justice*, Valencia: Tirant Lo Blanch, 2021, 728
- BLANCO CORDERO, Isidoro, «La menor edad como fundamento de la agravación de la pena: estudio crítico de los tipos agravados por razón de la menor edad y la especial vulnerabilidad», in Clara MOYA GUILLEM; Dyango BONSIGNORE FOUQUET, ed., *La protección de las víctimas especialmente vulnerables: Aspectos penales, procesales y político-criminales*, Valencia: Tirant lo Blanch, 2023, 121-160.
- BORGES BLÁZQUEZ, Raquel, «Inteligencia artificial y perspectiva de género en el proceso penal: una asignatura pendiente», in César VILLEGAS DELGADO; Maria del Pilar MARTÍN RÍOS, ed., *El Derecho de la Encrucijada Tecnológica: Estudios sobre Derechos Fundamentales, nuevas tecnologías e inteligencia artificial*, Valencia: Tirant lo Blanch, 2022, 281-299.
- BORGES BLÁZQUEZ, Raquel, «Sistemas de inteligencia artificial y policía predictiva: sweetie y la lucha contra la pedofilia», *La Ley Probática*, 7 (2022).
- DE SANTISTEBAN, Patricia; GÁMEZ-GUADIX, Manuel, «Online grooming y explotación sexual de menores a través de internet», *Revista de Victimología* [em linha], 6 (Ejemplar dedicado a: Revista de Victimología / Journal of Victimology) (2017) 81-100, [consult. 1 Jun. 2024]. Disponível em: <<https://dialnet.unirioja.es/servlet/articulo?codigo=6235522>>.
- DOLZ LAGO, Manuel Jesús, «Una aproximación a la inteligencia artificial», *Diario La Ley*, 10096 (2022) 1-40.
- ETXEBERRIA GURIDI, José Francisco, «Sistemas biométricos y su aplicación», in Silvia BARONA VILAR, ed., *Justicia poliédrica en periodo de mudanza: nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad*, Valencia: Tirant lo Blanch, 2022, 455-482.
- FERNÁNDEZ SENAC, Gloria, «La victimización sexual online en mujeres adolescentes y jóvenes», in Alejandro GARCÍA PEÑA; Helena SOLETO MUÑOZ; Aurea GRANÉ CHÁVEZ, ed., *El sistema de justicia ante la victimización sexual*, Madrid: Dykinson, 2023, 630-673.
- GONZÁLEZ-ÁLVAREZ, José Luis; SANTOS HERMOSO, Jorge; CAMACHO-COLLADOS, Miguel, «Policía predictiva en España: Aplicación y retos futuros», *Behavior & Law Journal* [em linha], 6/1 (2020) 26-41, [consult. 14 Jun. 2024]. Disponível em: <<https://www.behaviorandlawjournal.com/BLJ/article/view/75/90>>.
- GUARDIOLA SALMERÓN, Miriam, «Menores y redes sociales: nuevos desafíos jurídicos», *Revista de Derecho, Empresa y Sociedad (REDS)* [em linha], 8 (2016) 53-67, [consult. 14 Ag. 2024]. Disponível em: <<https://dialnet.unirioja.es/servlet/articulo?codigo=6140097>>.
- GUTIÉRREZ AZANZA, Diego Alberto, «Delito de “child grooming”: configuración jurisprudencial», *La Ley Derecho de Familia: Revista jurídica sobre familia y menores*, 27 (2020) 1-9.
- LÓPEZ GRANDE, Carlos Edgardo; SALVADOR GUADRÓN, Ricardo, «Ingeniería social: el ataque silencioso», *Revista Tecnológica* [em linha], 8 (Jan. 2015) 38-45, [consult. 19 Maio 2024]. Disponível em: <<https://core.ac.uk/download/pdf/80296691.pdf>>.
- LÓPEZ PÉREZ, Tatiana, «Policía predictiva (predictive police)», in Sonia CALAZA LÓPEZ; Mercedes LLORENTE SÁNCHEZ-ARJONA, ed., *Inteligencia artificial legal y Administración de Justicia* [em linha], Aranzadi:

- Thomson Reuters, 2022, 567-572, [consult. 23 Maio 2024]. Disponível em: <<https://dialnet.unirioja.es/servlet/libro?codigo=870011>>.
- MAGRO SERVET, Vicente, «Cómo prevenir la sextorsion y cómo se sancionan los ataques sexuales on line tras la Ley Orgánica 4/2023 de 27 de abril», *Diario La Ley*, 10290 (2023) 1-11.
- MARTÍN DIZ, Fernando, «Justicia predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria», in Federico BUENO DE MATA, ed., *El impacto de las tecnologías disruptivas en el Derecho Procesal*, Aranzadi: Thomson Reuters, 2022, 131-154.
- «Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria», in Silvia BARONA VILAR, ed., *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, Valencia: Tirant lo Blanch, 2021, 65-85.
- MARTÍNEZ VÁZQUEZ, Francisco, «El uso ilícito del ciberespacio en la crisis del COVID-19», *La Ley Privacidad*, 4 (Dedicado a: Lecciones aprendidas desde el confinamiento: abril-junio) (2020) 1-14.
- MÉNDEZ, Layssa; PÉREZ FERNÁNDEZ, Francisco, «El grooming como factor de impacto en tiempo de pandemia», *Diario La Ley*, 9752 (2020) 1-10.
- MUÑOZ RODRÍGUEZ, Ana Belén, «El impacto de la inteligencia artificial en el proceso penal», *Anuario de la Facultad de Derecho. Universidad de Extremadura* [em linha], 16 (2020) 695-728, [consult. 16 Mar. 2024]. Disponível em: <<https://dialnet.unirioja.es/download/articulo/7849592.pdf>>.
- ORTEGO PÉREZ, Francisco, «Investigación y prueba digital de los ciberdelitos», *Justicia: Revista de Derecho Procesal* [em linha], 2 (2022) 89-132, [consult. 28 Jun. 2024]. Disponível em: <<https://vlex.es/vid/investigacion-prueba-digital-ciberdelitos-924077816>>.
- RODRÍGUEZ LAINZ, José Luis, «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», in Inmaculada LÓPEZ-BARAJAS PEREA; Manuel DÍAZ MARTÍNEZ, ed., *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Valencia: Tirant lo Blanch, 2018, 17-48.
- RODRIGUEZ TIRADO, Ana María, «Las víctimas menores de delitos de pornografía infantil y de delitos de child grooming y su protección en el proceso penal: Las TICs y las diligencias de investigación tecnológica», *Justicia: Revista de Derecho Procesal* 1 (2018) 137-200.
- SAN MIGUEL CASO, Cristina, «Desafíos y propuestas sobre la aplicación de la inteligencia artificial en el proceso penal», in José Ignacio SOLAR CAYÓN; Maria Olga SÁNCHEZ MARTÍNEZ, ed., *El impacto de la inteligencia artificial en la teoría y la práctica jurídica*, [S.l.]: Wolters Kluwer España, Wolters Kluwer Legal & Regulatory España, 2022, 299-316.