Doble grau en Criminologia i Polítiques Públiques de Prevenció i Dret

Treball de Fi de Grau (21067/22747)

Curs acadèmic 2023-2024

LA INTEL·LIGÈNCIA ARTIFICIAL I EL SEU IMPACTE EN LA VIOLÈNCIA MASCLISTA: *EL CAS DELS DEEPFAKES.*

Lydia Galindo Puche

NIA 229616

Tutora del treball:

Beatriz Goena Vives

DECLARACIÓ D'AUTORIA I ORIGINALITAT

Jo, Lydia Galindo Puche, certifico que el present treball no ha estat presentat per a l'avaluació de cap altra assignatura, ja sigui en part o en la seva totalitat. Certifico també que el seu contingut és original i que en sóc l'únic/a autor/a, no incloent cap material anteriorment publicat o escrit per altres persones llevat d'aquells casos indicats al llarg del text.

Com a autora de la memòria original d'aquest Treball Fi de Grau autoritzo la UPF a dipositar-la i publicar-la a l'e-Repositori: Repositori Digital de la UPF, http://repositori.upf.edu, o en qualsevol altra plataforma digital creada per o participada per la Universitat, d'accés obert per Internet. Aquesta autorització té caràcter indefinit, gratuït i no exclusiu, és a dir, sóc lliure de publicar-la en qualsevol altre lloc.

Lydia Galindo Puche

Mallorca, 16 de maig de 2024.

RESUM

La violència masclista ha patit una forta transformació els darrers anys: primer amb l'aparició de les tecnologies de la informació i la comunicació i, actualment, amb la irrupció de la Intel·ligència Artificial Generativa, donant com a resultat l'aparició dels *deepfakes* –també en la seva modalitat de *deepnudes*–. Aquests continguts d'imatge, vídeo, àudio o text són una eina de doble tall: tot i comportar alguns beneficis en la detecció delictiva i en matèria probatòria, suposen un nou espai per la comissió delictiva –ja que els *deepfakes* poden ser emprats per finalitats malicioses contra les seves víctimes, les quals majoritàriament són dones–. Enfront de l'auge d'aquesta situació tan recent i escassa de regulació, es posa de manifest la necessitat de dur a terme propostes per normativitzar un fenomen que comporta un greu impacte en la vida de les víctimes. Concretament, se sostén com a opció més adequada la creació d'un tipus penal específic que penalitzi els *deepfakes* com a delicte contra la integritat moral. Així mateix, es fan propostes perquè les autoritats judicials constin de preparació suficient per abordar un tema tan complex i nou.

Paraules clau: Ciberviolència masclista, intel·ligència artificial generativa, *deepfakes*, ciberdelinqüència, xarxes socials.

ABSTRACT

In recent years, violence against women has undergone a strong transformation: firstly, with the emergence of information and communication technology and, currently, with the impact of Generative Adversarial Networks, resulting in the emergence of deepfakes –and also in its deepnude modality–. These images, videos, audios or text contents are a double-edged tool: despite bringing some benefits in criminal detection and in matters of evidence, it is a new space to commit crimes –since deepfakes can be used for malicious purposes against their victims, who are mostly women–. Facing the rise of this very recent and barely regulated situation, the need to make proposals to regulate a phenomenon that entails a serious impact on the lives of its victims is highlighted. Specifically, it has been considered as the most appropriate option to create a specific criminal type that penalizes deepfakes as a crime against moral integrity. Likewise, proposals are made so that the judicial authorities have sufficient preparation to address such a complex and new issue.

Keywords: *cyber violence against women, Generative Adversarial Networks, deepfakes, cybercrime, social networks.*

Para tí, papá, porque sé que a cada paso que dé,
siempre estarás guiándome.

A tí, mamá, por ser la fuerza que me lleva. Gracias,
por hacerme la mujer que soy.

A en Joan, per haver compartit aquesta etapa de la mà.
El teu suport incondicional ha fet el camí més fàcil.

ÍNDEX

1- INTRODUCCIÓ

L'existència de la violència masclista en la nostra societat és un fenomen latent que s'arrossega des d'èpoques passades; malgrat això, és un tipus de violència en constant procés de metamorfosi. El present treball pretén abordar precisament la transformació de la violència masclista –sempre des d'una perspectiva de gènere–: primer, a causa de l'aparició de les tecnologies de la informació i la comunicació (d'ara endavant, TIC) –les quals donen lloc a la ciberviolència masclista–; i, actualment, per la irrupció de la Intel·ligència Artificial (d'ara endavant, IA) en aquest àmbit –amb el sorgiment dels anomenats *deepfakes*–.

L'interès pel present treball deriva en l'actualitat del tema exposat i, en conseqüència, en la seva escassa regulació. La falta d'un marc regulador específic enfront de l'increment dels casos de *deepfake* i l'impacte eticomoral d'aquests presenten un panorama d'incertesa tant social com jurídica. És per aquest fet que al treball s'estudia el fenomen i s'avaluen les possibles controvèrsies juridicolegals per poder fer propostes per la seva necessària regulació.

En primera instància, es conceptualitza la ciberviolència masclista –matisant l'elecció del terme violència masclista enfront d'altres, per ser un concepte més plural i ampli–, la seva evolució i els tipus més rellevants i, tot seguit, es fa una anàlisi legislativa de la ciberviolència masclista; aquests punts es relacionen mitjançant una taula d'elaboració pròpia que classifica els tipus de ciberviolència masclista segons el bé jurídic a protegir i el tipus penal en què s'insereix o en què es podrien inserir. Així mateix, s'exposen dades estadístiques respecte a la ciberviolència masclista a Espanya per emfatitzar la magnitud i l'impacte del fenomen.

Segonament, es tracta la transformació de la ciberviolència masclista a causa de l'aparició de la IA on es fa una breu aproximació al concepte d'IA –destacant la IA generativa, en la qual tenen cabuda els *deepfakes*– així com del concepte de *deepfake,* les seves finalitats, la modalitat de *deepnude* i el seu impacte –a través d'estadístiques i casos mediàtics–*;* així mateix, es posa de manifest l'existència del Reglament d'IA aprovat a la Unió Europea i la falta de regulació nacional –tot i l'existència d'una Proposició de Llei Orgànica al respecte–.

En tercer lloc, es duen a terme dos tipus de propostes enfront de l'estat de la fenomenologia: una proposta de *lege ferenda* per regular a escala estatal els *deepfakes,* optant per la seva penalització en un tipus específic del Codi Penal, en concret com a delicte contra la integritat moral; d'altra banda, propostes per la preparació de jutges i fiscals enfront d'aquests casos.

2- LA CIBERVIOLÈNCIA MASCLISTA: CONCEPTE I GÈNESI

1) Aclariment terminològic de la violència masclista.

Com a qüestió prèvia, és necessari precisar el concepte **"violència masclista",** entès com a sinònim del concepte "violència contra les dones" utilitzat en els principals tractats internacionals en la matèria subscrits per Espanya. En aquest sentit, en la Declaració sobre l'Eliminació de la Violència contra la Dona, de 20 de desembre de 1993, de l'Assemblea General de les Nacions Unides s'entén per violència contra les dones *"tot acte de violència basat en la pertinença al sexe femení que tingui o pugui tenir per resultat un dany o patiment físic, psicològic o sexual per a les dones, així com les amenaces de tals actes, la coacció o la privació arbitrària de la llibertat, tant si es produeixen a la vida pública com a la privada"*.[1]

No obstant això, la Llei Orgànica 1/2004, de 28 de desembre, de Mesures de Protecció Integral contra la Violència de Gènere –d'ara endavant LOMPIVG– inclou indirectament aquest concepte en l'apartat primer de l'exposició de motius, determinant que: *"La violència de gènere no és un problema que afecti l'àmbit privat. Per contra, és manifesta com el símbol més brutal de la desigualtat existent a la nostra societat. Es tracta d'una violència que es dirigeix sobre les dones pel fet mateix de ser-ho, perquè són considerades, pels seus agressors, mancades dels drets mínims de llibertat, respecte i capacitat de decisió"*. Aquesta afirmació –que encaixaria amb el terme de violència masclista– queda matisada en l'art. 1 LOMPIVG, establint-se que només es donarà quan aquests siguin o hagin estat cònjuges o de qui estiguin o hagin estat lligats a elles per relacions similars d'afectivitat, tot i no haver-hi convivència.[2] Per tant, la violència masclista és un concepte més plural que el de violència de gènere pel fet que es pot manifestar en diferents àmbits, com són el de la parella (violència de gènere), familiar (violència intrafamiliar o vicària), digital (ciberviolència masclista), laboral, social, comunitari, institucional, vida política i esfera pública de les dones, educatiu i altres formes que lesionin o puguin lesionar la dignitat, integritat i llibertat de les dones.[3]

---

[1] Secretaría General del Congreso de los Diputados (2021). Registro General. Entrada 79830. https://www.congreso.es/entradap/l14p/e7/e_0079830_n_000.pdf

[2] Llorens, M. (2022) "Avances legislativos y retos en materia de violencia de Género Digital". *Nuevas tecnologías 2022,* 231-248. Tirant lo Blanch.

[3] Departament d'Interior de la Generalitat de Catalunya (s.d.), *Violència masclista.* https://interior.gencat.cat/es/arees_dactuacio/seguretat/violencia_masclista/

2) La ciberviolència masclista: concepte i tipus.

Les conductes anteriorment citades traslladades als mitjans tecnològics produeixen una amplificació del fenomen sobre la víctima que es pot arribar a sentir atrapada en qualsevol espai –l'analògic *(offline)* i el digital *(online)*–,[4] ja que el ciberespai ofereix a l'agressor noves vies per reafirmar el seu domini i exercir violència a distància.[5] La Fiscalia General de l'Estat, a la Memòria del 2021, assenyala que "*les possibilitats que ofereixen les TIC per difondre tota mena de continguts estan determinant que es reflecteixin al ciberespai les mateixes desigualtats i factors discriminatoris que es detecten a l'entorn físic, circumstància afavorida per la bretxa digital de gènere, com a factor que contribueix a reproduir i perpetuar al ciberespai les diferències i asimetries ja preexistents entre homes i dones"*.[6] Per tant, la majoria d'aquestes formes de violència contra les dones ja existien fora de línia, sent crims i delictes existents ampliats o generalitzats per Internet i les tecnologies digitals[7] a causa de les facilitats que aporta l'entorn digital: la desinhibició *online*, possibilitat d'obtenció de moltes dades de la víctima –intimitat accelerada–, l'anonimat,[8] la falsa sensació d'impunitat, el fàcil accés i la immediatesa, permanència i exposició.[9] En conseqüència, el Consell d'Europa va definir la ciberdelinqüència com *"l'ús de sistemes informàtics per causar, facilitar o amenaçar amb violència contra les persones, que té com a resultat, o pot tenir com a resultat, un dany o patiment físic, sexual, psicològic o econòmic, i pot incloure l'explotació de la identitat de la persona, així com de les circumstàncies, característiques o vulnerabilitats de la persona"*.[10]

Concretament, dins l'àmbit digital de la violència masclista s'emmarca el concepte de **ciberviolència masclista**, al qual es farà referència al llarg del present treball per abordar la diversitat terminològica existent, per exemple: violència de gènere digital, ciberviolència de gènere, violència digital o *online*, e-violència de gènere, violència 2.0, entre d'altres. Igual

[4] Sala, R. (2019). "La violencia de género digital: tratamiento jurídico y percepción social". *La Ley Derecho de Familia: Revista jurídica sobre familia y menores,* (23), 34-40.
[5]Martín, R. (2021). "Violencia de género en la era digital: el delito de sexting". *Feminismo digital: violencia contra las mujeres y brecha sexista en Internet,* 421-439.
[6] Fiscalía General del Estado. (2022) Memoria de la Fiscalía General del Estado 2021. Ministerio de Justicia.
[7] Van der Wilk, A. (2021). *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología.* Consejo de Europa.
[8] Lloria, P. (2014). "Violencia de género en el entorno digital". *Crímenes y castigos: miradas al Derecho penal a través del arte y la cultura*, 547-562. Tirant lo Blanch.
[9] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).
[10] Consejo de Europa (2018). Mapping study on cyberviolence. Cybercrime Convention Committee (TCY). Working Group on cyberbullying and other forms of violence, especially against women and children.

que no existeix cap terminologia globalment acceptada, tampoc hi ha una definició unificada d'aquest tipus de violència, ni a escala europea ni a escala estatal:[11] a Europa, el concepte és més ampli, ja que no només inclou la parella o l'exparella –a diferència del que es preveu a Espanya– sinó que l'autor podria ser qualsevol home i la víctima qualsevol dona –amb vincle d'afecte o sense–. S'opta llavors pel concepte de ciberviolència masclista per ser més ampli que el de violència digital de gènere i permetre englobar més tipus de violències, com les violències interseccionals (per raó d'ètnia, classe, diversitat funcional, expressió de gènere, cossos dissidents, etc.) o tipus com el ciberassetjament, la pornografia no consentida, els insults i l'assetjament per motius de gènere, la pràctica de titllar de prostituta, l'extorsió sexual i el *doxing*, entre d'altres.[12] Tenint en compte aquest fet, es podria definir la ciberviolència masclista com totes les conductes de violència que es perpetuen per raons de gènere dins el ciberespai a través de les noves tecnologies, les xarxes socials o Internet,[13] donant-se un trasllat de les violències masclistes a la realitat *online*, a on es digitalitzen les situacions violentes, intimidatòries i mecanismes de control.[14] Ara bé, no es tracta només de dur a terme conductes de control i humiliació a través de les TIC, sinó d'un canvi profund que situa el dret d'imatge, l'honor i intimitat en primera línia de l'atac masclista.[15] Per tant, comprèn els delictes comesos a través d'Internet per raó de gènere prevalent-se l'agressor de l'abast i l'especial lesivitat dels mitjans tecnològics, tant a l'àmbit públic com privat, amb independència de la relació preexistent amb la víctima.[16]

Com s'ha anat apuntant, són diverses les tipologies que conformen el fenomen de la ciberviolència masclista, no obstant això, pel present treball es consideraran com a principals formes d'aquest tipus de violència les exposades a continuació.

---

[11] European Parliamentary Research Service (2021). *Combating gender-based violence: Cyber violence European added value assessment.* European Parliament.

[12] Instituto Europeo de Igualdad de Género (2017). *La ciberviolencia contra mujeres y niñas.* Oficina de Publicaciones de la Unión Europea, 1-11.

[13]Delegación del Gobierno contra la Violencia de Género. (s.d.) *Violencia de género digital.* Disponible a: https://violenciagenero.igualdad.gob.es/informacionUtil/comoDetectarla/VG_Digital/home.htm. En el mismo sentido Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).

[14] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).

[15] Gavilán, M. (2018). "Violencia de género digital: el delito de ciberacoso. Breve resumen de jurisprudencia. Asistencia a la víctima". *Servicios sociales y política social*, (116), 53-61.

[16]González, I. (2023) "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes". *IUS ET SCIENTIA,* 9 (2), 157-180.

Comprenen el **ciberassetjament (*cyberstalking*) per raó de violència masclista** els comportaments que utilitzant les TIC tenen com a objectiu la dominació, discriminació i abús de la posició de poder on l'home assetjador té o ha tingut alguna relació afectiva o de parella amb la dona assetjada; aquest assetjament ha de ser repetitiu, no consentit, ha de suposar una intromissió a la vida privada de la víctima i, el motiu d'aquest assetjament, ha d'estar relacionat en alguna mesura amb la relació afectiva que tenen o van tenir assetjador i assetjada.[17] Cal diferenciar el **ciberassetjament sexista** del **ciberassetjament sexual**.

El primer abastaria actituds, verbalitzacions o comportaments que es produeixin a les TIC i que se sustentin en estereotips de gènere (com insults o agressions dirigides a la imatge corporal).[18] Dins aquesta categoria es poden inserir conductes com el ***body-shaming (o fat-shaming)*** que il·lustra la pràctica d'humiliar una dona per no ajustar-se als cànons de bellesa que estableix la norma heteropatriarcal social;[19] a través de les xarxes es manifesten les crítiques, agressions i burles, atemptant contra l'autoestima de la persona.[20] També es pot incloure el conegut com a ***slut-shaming,*** el qual es basa en titllar de puta i humiliar una dona –en tot l'aspecte del seu desenvolupament digital– pels seus comportaments o desitjos sexuals que s'allunyen dels que la norma heteropatriarcal estableix per al sexe femení. Finalment, també englobaria la **cibermisogínia,** consistent en l'insult virtualitzat que a través de la generalització tracta de reproduir odi sobre les dones o subjectes feminitzats.[21]

En canvi, en el ciberassetjament sexual s'emmarquen les actituds, verbalitzacions i comportaments sexuals que es produeixen a les TIC amb efecte d'atemptar contra la dignitat d'una noia, en particular quan es crea un entorn intimidatori, degradant o ofensiu (per exemple, l'enviament i difusió d'imatges i/o vídeos íntims sense el seu consentiment).[22]

És important desvincular el ***sexting*** del ciberassetjament sexual, ja que és una pràctica desitjada i realitzada de forma lliure, autònoma i consensuada en què es comparteixen fotos,

---

[17] Torres, C., Robles, J.M. i de Marco, S. (2014). *El ciberacoso como forma de ejercer la violencia de género en la juventud: Un riesgo en la sociedad de la información y el conocimiento.* Ministerio de Sanidad, Servicios Sociales e Igualdad.

[18] Rodríguez, J. & Rodríguez, L. (2022). "Violencia de género en soportes digitales". *Opción: Revista de Ciencias Humanas y Sociales*, (29), 396-416.

[19] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).

[20] Rodríguez, J. & Rodríguez, L. (2022). "Violencia de género en soportes digitales". *Opción: Revista de Ciencias Humanas y Sociales*, (29), 396-416.

[21] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).

[22] Linares, E.; Royo, R.; Silvestre, M. (2019). "El ciberacoso sexual y/o sexista contra las adolescentes. Nuevas versiones online de la opresión patriarcal de las sexualidades y corporalidades femeninas". *Doxa Comunicación,* 28, 201-222.

vídeos o textos sexualitzats a través del telèfon, amb l'objectiu principal de cercar gaudi.[23] Aquesta pràctica es torna problemàtica quan falla el consentiment en la presa o difusió de les imatges,[24] donant lloc a tipologies diverses de ciberviolència masclista. D'una banda, el **delicte de difusió aliena de *sexting* (*sexting* secundari)** està tipificat en l'art. 197.7 del Codi Penal (CP) i consisteix en la difusió, revelació o cessió a tercers d'imatges o gravacions de la víctima sense autorització d'aquesta, però obtingudes amb la seva anuència en un domicili o lloc fora de l'abast de la mirada de tercers quan aquesta divulgació menyscabi greument la seva intimitat; també és conegut com a **pornografia no consentida (*revenge porn*)** pel fet que es pot donar quan una persona, en forma de "venjança", difon el material d'una altra en acabar una relació (darrer incís art. 197.7 CP).[25] D'altra, la **sextorsió (extorsió sexual)** és una forma d'explotació sexual en què algú pateix xantatge amb una imatge o vídeo de si mateixa nua o fent actes sexuals, que en general han estat prèviament compartits mitjançant *sexting*; la víctima és coaccionada per tenir relacions sexuals, entregar més imatges eròtiques o pornogràfiques, diners o altres, sota l'amenaça de difusió de les imatges.[26]

El **cibercontrol** cap a les noies és el control constant de la persona amb qui es té un vincle afectiu i/o sexual a través dels mòbils (per exemple: demanar foto d'amb qui està, enviar la ubicació, apps de geolocalitzadors, controlar com utilitza les seves xarxes socials, demanar comprovants del que li diu és veritat…).[27] Amb freqüència hi ha connexió amb l'assetjament i quan la noia no respon al control que es pretén fer sobre ella la pot amenaçar amb la difusió de continguts o secrets. [28]

L'***online grooming*** és l'assetjament o apropament a un menor exercit per un adult amb fins sexuals a través d'accions realitzades deliberadament per establir una relació i control

[23] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).
[24] Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret*, 493-515.
[25] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).
[26] Martínez, M. I. (2015) "Las nuevas tecnologías como herramientas de prevención y actuación frente a la violencia de género". *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención,* 111-226. Universidad Internacional de Andalucía.
[27] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).
[28] Estebánez, I. (2018) *La ciberviolencia hacia las adolescentes en las redes sociales: guía didáctica.* Instituto Andaluz de la Mujer.

emocional sobre un nen o nena per tal de preparar el terreny per a l'abús sexual, incloent-hi des del contacte físic fins a les relacions virtuals i l'obtenció de pornografia infantil.[29]

Finalment, el ***doxing*** consisteix en l'extracció i la publicació no autoritzada d'informació personal, com per exemple: nom complet, adreça, telèfon, correu electrònic, familiars i fills, detalls financers o laborals, com una forma d'intimidació o amb la intenció de localitzar la persona al "món real" per assetjar-la. Aquesta informació també pot ser publicada a llocs pornogràfics juntament amb l'anunci del fet que la víctima està oferint serveis sexuals.[30]

3) Anàlisi legislativa de la ciberviolència masclista.

A escala europea, l'Avaluació Europea de Valor Afegit *"Combating gender-based violence: cyber violence"* publicada l'abril del 2021, constata l'àmplia falta d'accions legals per part de la Unió Europea en la matèria. A la Unió Europea no existeix un enfocament únic per combatre la ciberviolència, ni tampoc hi ha cap escenari legal que ataqui directament la ciberviolència masclista. Malgrat això, el Consell d'Europa compta amb diversos tractats i protocols com el Conveni de Budapest sobre la Ciberdelinqüència, el Conveni d'Istanbul per prevenir i combatre la violència contra les dones i la violència domèstica[31] i el Conveni de Lanzarote per la Protecció de la Infància contra l'Explotació Sexual i Abús Sexual.[32]

Vers l'àmbit regulador espanyol cal destacar que al preàmbul de la LOMPIVG s'estableix que la violència masclista és un dels atacs més flagrants dels drets fonamentals com la llibertat, la igualtat, la vida, la seguretat i la no discriminació proclamats en la Constitució Espanyola de 1978.

El legislador al Codi Penal no ha diferenciat en un títol apartat els ciberdelictes, sinó que a les conductes delictives existents afegeix noves modalitats. Amb relació als delictes de ciberviolència masclista, alguns preceptes no indiquen explícitament l'ús de noves

[29] Duque, I. (2020) *Guía didáctica. Conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).
[30] Vera, K. (2021). *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos.* OAS Documentos oficiales.
[31] Cal destacar que tot i que el Conveni d'Istambul no conté referència explícita a la dimensió digital de violència contra les dones, el seu àmbit d'aplicació, tal com està definit en l'art 2, abarca la violència en l'espai digital. Van der Wilk, A. (2021). *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología.* Consejo de Europa.
[32] Llorens, M. (2022) "Avances legislativos y retos en materia de violencia de Género Digital". *Nuevas tecnologías 2022,* 231-248. Tirant lo Blanch.

tecnologies, però inclouen accions com revelar o difondre, les quals es poden fer a través de mitjans telemàtics –per tant, no es pot dir que hi hagi delictes que per definició siguin ciberviolència masclista, però sí susceptibles d'adquirir aquesta condició–. Destaquen l'art. 197 CP respecte de conductes que lesionen la intimitat personal, familiar i pròpia imatge de la víctima i els arts. 183 ter i 189 b) CP sobre conductes relacionades a abusos sexuals en la xarxa, en especial quan es tracta de menors; respecte de les conductes d'amenaces destaca l'art. 171.2 CP i, amb relació a les conductes d'enaltiment a l'odi l'art. 510 CP.[33]

La recent Llei Orgànica 10/2022, de 6 de setembre, de garantia integral de la llibertat sexual indica al seu preàmbul que pretén donar resposta especialment a les violències sexuals comeses en l'àmbit digital, cosa que comprèn la difusió d'actes de violència sexual a través de mitjans tecnològics, la pornografia no consentida i l'extorsió sexual.[34] En relació, s'ha observat que en diferents articles s'inclou la comissió d'aquests actes en l'àmbit digital.

A escala autonòmica, pren rellevància la Llei 15/2021, de 3 de desembre, per la qual es modifica la Llei 11/2007, de 27 de juliol, gallega per a la prevenció i el tractament integral de la violència de gènere, ja que és la primera en territori nacional que inclou dins el seu àmbit de protecció a les dones que pateixen ciberviolència masclista[35]; per altra banda, la Llei 7/2018, del 30 de juliol, de Mesures de Prevenció i Protecció Integral Contra la Violència de Gènere d'Andalusia defineix la ciberviolència contra les dones a l'art. únic quart pel qual es modifica l'art. 3 de la Llei 13/2007, de 26 de novembre.[36]

En darrer terme, també cal tenir en compte la Llei Orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

4) Classificació dels tipus de ciberviolència masclista: bé jurídic i tipus penals.

Gràcies a les anteriors definicions i tenint en compte la regulació actual d'aquestes conductes, es realitza una possible classificació a tall de sintetitzar i categoritzar les anteriors conductes extrapenals –no tipificades al CP, a excepció del *sexting* secundari i l'*online grooming*–.

---

[33] *Ídem.*

[34] Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

[35] Llorens, M. (2022) "Avances legislativos y retos en materia de violencia de Género Digital". *Nuevas tecnologías 2022,* 231-248. Tirant lo Blanch.

[36] Ley 7/2018, de 30 de julio, por la que se modifica la Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género.

Mitjançant la següent taula es classifiquen els tipus de ciberviolència masclista tenint en compte el bé jurídic a protegir i tipus penal en què s'insereixen o es podrien inserir.

<table>
<tr><th colspan="4">CIBERASSETJAMENT SEXISTA

Actituds, verbalitzacions o comportaments que es produeixin a les TIC i que se sustentin en estereotips de gènere (per exemple insults o agressions dirigides a la imatge corporal). Es poden inserir el body-shaming (o fat-shaming), el slut-shaming, i la cibermisogínia.</th></tr>
<tr><th colspan="2">BREU DEFINICIÓ DE LES CONDUCTES QUE COMPRÈN</th><th>BÉ JURÍDIC A PROTEGIR</th><th>TIPUS PENAL EN QUÈ S'INSEREIX O ES PODRIA INSERIR LA CONDUCTA</th></tr>
<tr><td>Body-shaming (o fat-shaming)</td><td>Humiliar una dona per no ajustar-se als cànons de bellesa que estableix la norma heteropatriarcal social. A través de les xarxes es manifesten les crítiques, agressions i burles, atemptant contra l'autoestima.</td><td rowspan="3">Dret a l'honor i dret a la integritat moral.</td><td rowspan="3">Es podria inserir en els arts. 208 a 210 del Codi Penal (CP) sobre les injúries pel fet que es tracta d'expressions que lesionen la dignitat de l'altra persona, menyscabant la seva fama o atemptant contra la seva pròpia estimació, quan aquestes siguin considerades com a greus.

També és possible incloure'l en l'art. 173.1 CP respecte dels delictes contra la integritat moral perquè amb aquestes conductes s'infligeix a una altra persona un tracte degradant, menyscabant greument la seva integritat moral. Cal destacar l'art. 173.4 CP, ja que es castiga a aquell que causi injúria o vexació injusta de caràcter lleu, quan l'ofès sigui una de les persones de l'art. 173.2 CP (inclou qui sigui o hagi estat cònjuge o persona lligada per anàloga relació d'afectivitat tot i sense convivència). També es pot castigar a través de l'art. 173.4 II CP, el qual imposa penes a qui es dirigeixi contra una altra persona amb expressions, comportaments o proposicions de caràcter sexual que creïn a la víctima una situació objectivament humiliant, hostil o intimidatòria sense arribar a constituir altres delictes de major gravetat.

La cibermisogínia també es podria inserir en l'art. 510 CP respecte als delictes d'odi, ja que castiga al que públicament fomenti, promogui o inciti directament o indirectament a l'odi, hostilitat, discriminació o violència contra un grup, una part d'aquest o contra una persona determinada per raó de la seva pertinença d'aquell per (...) el seu sexe. En aquest cas no es diu explícitament que la publicitat dels actes sigui a través de les xarxes socials, però es podria inferir aquesta possibilitat.</td></tr>
<tr><td>Slut-shaming</td><td>Titllar de puta i humiliar una dona –en tot l'aspecte del seu desenvolupament digital– pels seus comportaments o desitjos sexuals que s'allunyen dels que la norma heteropatriarcal estableix per al sexe femení.</td></tr>
<tr><td>Cibermisogínia</td><td>Insult virtualitzat que a través de la generalització tracta de reproduir odi sobre les dones o subjectes feminitzats.</td></tr>
<tr><th colspan="4">CIBERASSETJAMENT SEXUAL

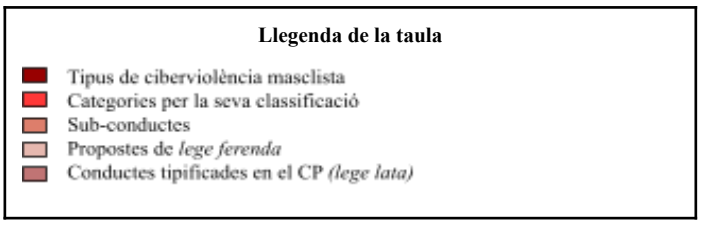
Actituds, verbalitzacions i comportaments sexuals que es produeixen a les TIC amb efecte d'atemptar contra la dignitat d'una noia, en particular quan es crea un entorn intimidatori, degradant o ofensiu (per exemple, l'enviament i difusió d'imatges i/o vídeos íntims sense el seu consentiment). Dins aquest trobem conductes com el sexting secundari, la pornografia no consentida o la sextorsió.</th></tr>
<tr><th colspan="2">BREU DEFINICIÓ DE LES CONDUCTES QUE COMPRÈN</th><th>BÉ JURÍDIC A PROTEGIR</th><th>TIPUS PENAL EN QUÈ S'INSEREIX O ES PODRIA INSERIR LA CONDUCTA</th></tr>
<tr><td>Sexting secundari (difusió aliena de sexting) i revenge porn (pornografia no consentida)</td><td>Difusió, revelació o cessió a tercers d'imatges o gravacions de la víctima sense la seva autorització, però obtingudes amb la seva anuència en un domicili o lloc fora de l'abast de la mirada de tercers quan aquesta divulgació menyscabi greument la seva intimitat. També és conegut com a pornografia no consentida (revenge porn) pel fet que es dona a vegades quan una persona, en forma de "venjança", difon el material d'una altra en acabar una relació.</td><td>Dret a la intimitat i dret a la pròpia imatge.</td><td>Es troba tipificat en l'art. 197.7 CP, des de la reforma del CP a través de la LO 1/2015 de 30 de març per la qual es modifica la LO 10/1995 de 23 de novembre, del Codi Penal. El revenge porn està tipificat en concret en el darrer incís de l'art. 197.7 CP.</td></tr>
<tr><td>Sextorsió (Extorsió sexual)</td><td>Forma d'explotació sexual en què una persona pateix el xantatge part d'una altra amb una imatge o vídeo de si mateixa nua o realitzant actes sexuals, que generalment han estat prèviament compartits mitjançant sexting; la víctima és coaccionada per tenir relacions sexuals amb algú, entregar més imatges eròtiques o pornogràfiques, diners o altres, sota l'amenaça de difusió de les imatges.</td><td>Dret a la llibertat, dret a la intimitat, dret a la pròpia imatge i dret a la integritat moral.</td><td>Es podria inserir en l'art. 169 CP respecte a les amenaces sobre causar-li a ella, a la seva família o altres persones amb qui estigui íntimament vinculat, un mal que constitueixi delictes d'homicidi, lesions, avortament, contra la llibertat, tortures i contra la integritat moral, la llibertat sexual, la intimitat, l'honor, el patrimoni i l'ordre socioeconòmic.

Respecte de les coaccions, en l'art. 172 CP el qual castiga aquell que sense estar llegítimament autoritzat, impedeixi a un altre amb violència a fer el que la llei no</td></tr>
</table>

			prohibeix o el compel·leixi a efectuar allò que no vol, sigui just o injust. També es castiga quan es coaccioni lleument a qui sigui o hagi estat la seva esposa o dona que estigui o hagi estat lligada a ell per anàloga relació d'afectivitat, tot i sense convivència. S'imposa la pena en la meitat superior si el delicte es perpetua en presència de menors o en el domicili comú/de la víctima o es trenqui una pena de l'art. 48 CP o mesura cautelar o de seguretat de la mateixa naturalesa. També en l'art. 187 CP respecte de l'explotació sexual i prostitució pel fet que es castiga aquell que emprant violència, intimidació o engany o abusant d'una situació de superioritat, necessitat o vulnerabilitat de la víctima, determini a algú major d'edat exercir o mantenir-se en la prostitució. Es castiga a qui es lucra explotant la prostitució d'una altra persona, tot i el consentiment d'aquesta. Es considera explotació quan la víctima està en situació de vulnerabilitat personal/econòmica i se li imposin condicions gravoses, desproporcionades o abusives. Les penes s'imposen sense perjudici de les que corresponguin per agressions o abusos sexuals comesos sobre la persona prostituïda. Cal destacar l'art. 188 CP, el qual castiga les anteriors conductes respecte menors o persones amb discapacitat. Així mateix, en l'art 197.7 CP perquè fa referència a aquell que sense autorització de l'afectada difongui, reveli o cedeixi a tercers imatges o gravacions audiovisuals d'aquella que hagués obtingut amb la seva anuència en un domicili o en qualsevol altre lloc fora de l'abast de la mirada de tercers, quan la divulgació menyscabi greument la intimitat personal d'aquesta persona. Possibilitat d'incloure'l en l'art. 243 CP sobre l'extorsió, tot i que amb modificacions d'aquest article, ja que es castiga aquell que amb ànim de lucre obligui a altre, amb violència o intimidació a fer/ometre un acte o negoci jurídic en perjudici del seu patrimoni i del d'un tercer. Finalment, possibilitat d'inserir-lo en l'art. 173.1 CP respecte dels delictes contra la integritat moral perquè amb aquestes conductes s'infligeix a una altra persona un tracte degradant, menyscabant greument la seva integritat moral.
CIBERCONTROL CAP A LES NOIES			
BREU DEFINICIÓ DE LA CONDUCTA		**BÉ JURÍDIC A PROTEGIR**	**TIPUS PENAL EN QUÈ S'INSEREIX O ES PODRIA INSERIR LA CONDUCTA**
Control constant de la persona amb qui es té un vincle afectiu i/o sexual a través dels mòbils (ex. demanar foto d'amb qui està, enviar la ubicació, apps de geolocalitzadors, controlar com utilitza les seves xarxes socials, demanar comprovants del que li diu és veritat…). Amb freqüència hi ha connexió amb l'assetjament i quan la noia no respon al control que es pretén fer sobre ella la pot amenaçar amb la difusió de continguts o secrets.		Dret a la llibertat i dret a la intimitat.	Es podria inserir en l'art 172 ter CP, ja que fa referència a l'assetjament insistent reiterat, no autoritzat i que alteri el normal desenvolupament de la vida quotidiana quan la vigili, persegueixi o cerqui proximitat física o atempti contra la seva llibertat i patrimoni (o contra la llibertat o patrimoni d'algú proper a ella). En el cas que s'arribi a amenaçar-la, es podria incloure en l'art. 169 CP respecte a les amenaces sobre causar-li a ella, a la seva família o altres persones amb qui estigui íntimament vinculat, un mal que constitueixi delictes d'homicidi, lesions, avortament, contra la llibertat, tortures i contra la integritat moral, la llibertat sexual, la intimitat, l'honor, el patrimoni i l'ordre socioeconòmic.
ONLINE GROOMING			
BREU DEFINICIÓ DE LA CONDUCTA		**BÉ JURÍDIC A PROTEGIR**	**TIPUS PENAL EN QUÈ S'INSEREIX O ES PODRIA INSERIR LA CONDUCTA**
Assetjament o apropament a un menor exercit per un adult amb fins sexuals a través d'accions realitzades deliberadament per establir una relació i control emocional sobre un nen/a per tal de preparar el terreny per a l'abús sexual, incloent-hi des del contacte físic fins a les relacions virtuals i l'obtenció de pornografia infantil.		Dret a la llibertat i indemnitat sexual dels menors de 16 anys.	Es troba tipificat en l'art. 183 CP, introduït per la reforma 5/2010 de 22 de juny, per la qual es modifica la LO 10/1995, de 23 de novembre, del Codi Penal.

DOXING		
BREU DEFINICIÓ DE LA CONDUCTA	**BÉ JURÍDIC A PROTEGIR**	**TIPUS PENAL EN QUÈ S'INSEREIX O ES PODRIA INSERIR LA CONDUCTA**
Extracció i publicació no autoritzada d'informació personal, com per exemple: nom complet, adreça, telèfon, correu electrònic, familiars i fills, detalls financers o laborals, com una forma d'intimidació o amb la intenció de localitzar la persona al "món real" per assetjar-la. Aquesta informació també pot ser publicada a llocs pornogràfics juntament amb l'anunci del fet que la víctima està oferint serveis sexuals.	Dret a la llibertat, dret a la intimitat, dret a la integritat moral i dret a l'honor.	Possibilitat d'inserir-se en l'art 172 ter 1.3ª CP referent a l'assetjament insistent reiterat, no autoritzat i que alteri el normal desenvolupament de la vida quotidiana quan mitjançant l'ús indegut de les seves dades personals (...) faci que terceres persones es posin en contacte amb ella. S'imposa una pena de presó d'un a dos anys en cas que l'ofesa sigui o hagi estat cònjuge o amb qui estigui o hagi estat lligada per anàloga relació tot i sense convivència (art 173.2 CP). A més, l'art 172 ter 5 CP castiga a aquell que sense consentiment del titular utilitzi la imatge d'algú per fer anuncis o obrir perfils falsos a les xarxes socials, pàgines de contacte o qualsevol mitjà de difusió pública, ocasionant-li una situació d'assetjament, fustigació o humiliació. També es podria tipificar com delicte de l'art. 197 CP amb relació al descobriment o revelació de secrets per vulnerar la intimitat de l'altre sense el seu consentiment per qui s'apoderi de papers, cartes, missatges o altres documents o efectes personals o intercepti comunicacions (...) o qui sense estar autoritzat s'apoderi, utilitzi o modifiqui en perjudici de tercer dades reservades de caràcter personal o familiar registrats a fitxers o suports informàtics (...). Seria possible inserir-lo en l'art. 173.1 CP respecte dels delictes contra la integritat moral perquè amb aquestes conductes s'infligeix a una altra persona un tracte degradant, menyscabant greument la seva integritat moral. Cal destacar l'art. 173.4 CP, ja que es castiga a aquell que causi injúria o vexació injusta de caràcter lleu, quan l'ofès sigui una de les persones de l'art. 173.2 CP (inclou qui sigui o hagi estat cònjuge o persona lligada per anàloga relació d'afectivitat tot i sense convivència). Finalment, es podria inserir en els arts. 208 a 210 del Codi Penal (CP) quant a l'honor de la víctima en relació amb les injúries pel fet que es tracta d'expressions que lesionen la seva dignitat, menyscabant la seva fama o atemptant contra la seva pròpia estimació, quan aquestes siguin considerades com a greus.

Taula d'elaboració pròpia.



5) Magnitud del fenomen: dades estadístiques de la ciberviolència masclista a Espanya.

Segons les dades de l'Institut Nacional d'Estadística, l'any 2023 el 95,4% de les persones entre 16 i 74 anys van usar Internet en els darrers tres mesos i el 90% de forma diària. Per sexe, les dones presenten percentatges lleugerament superiors al dels homes.[37] En concordança amb aquestes xifres, la ciberdelinqüència també creix de forma exponencial: d'acord amb les estadístiques del Ministeri d'Interior, el percentatge que representa la

[37] Instituto Nacional de Estadística (2023). Notas de prensa. Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares Año 2023.

cibercriminalitat sobre el total d'infraccions penals va augmentant –d'un 7,5% el 2018 a un 16,1% el 2022–. Respecte als detinguts i investigats, un 71,9% són de sexe masculí i tenen lloc principalment per frau informàtic, delictes d'amenaces i coaccions i delictes sexuals; en canvi, pel que fa a les victimitzacions, les dones són més victimitzades en delictes contra l'honor (55%), delictes sexuals (68%) i descobriment i revelació de secrets (61%).[38] Segons dades de la Macroenquesta de Violència contra la Dona de 2019: el 7,4% de les dones de 16 anys o més han rebut algun cop insinuacions inapropiades, humiliants, intimidatòries o ofensives a través de les xarxes; un 18,4% han patit assetjament a través de les xarxes i un 7,2% han rebut imatges sexualment explícites; a més, un 15,2% de dones ha patit assetjament reiterat per part de la mateixa persona i entre aquestes, el 4,3% han experimentat com l'assetjador publicava fotos, vídeos o informació personal a les xarxes o l'enviava a tercers a través de serveis digitals; en addició, un 6,4% d'elles ha rebut assetjament a través de missatges escrits sexualment explícits. L'edat és un factor determinant que incrementa les possibilitats d'assetjament digital: de les dones entre 16 i 25 anys, més del 25% ha rebut insinuacions inapropiades a través de les xarxes i més del 20% ha rebut imatges, missatges o correus explícits. Referent a les victimitzacions per delictes sexuals contra les dones, aquestes han seguit una tendència creixent –de 223 el 2011 a 855 el 2020–. Posant èmfasi en tipus penals concrets, hi ha hagut un increment molt pronunciat de *grooming* envers les dones –passant de 0 a 328 casos entre 2011 i 2020– i de victimitzacions per abús sexual –de 23 a 113 casos–. Finalment, és necessari remarcar que malgrat les dades esmentades, la manca d'estadístiques específiques sobre aquest tipus de violència digital dificulta poder tenir una imatge clara del fenomen.[39]

3- L'APARICIÓ DE LA INTEL·LIGÈNCIA ARTIFICIAL: LA TRANSFORMACIÓ DE LA CIBERVIOLÈNCIA MASCLISTA.

1) Breu aproximació a la Intel·ligència Artificial: nocions bàsiques.

El terme **"Intel·ligència Artificial"** (d'ara endavant, IA) fou construït notòriament el 1955 en la Conferència de Dartmouth pel professor John McCarthy[40], tot i que els primers

[38]Muniesa, P.; Herrera, T.D.; Guerrero, J.; Martínez, F.; Rubio, M.; Gil, V.; Santiago, A.M. i Gómez, M.A. (2023). *Informe sobre la cibercriminalidad en España.* Ministerio del Interior.
[39]Observatorio Nacional de Tecnología y Sociedad (2022). *Violencia de género: una realidad invisible 2022.* Ministerio de Asuntos Económicos y Transformación Digital.
[40]López, S. (2023). "Inteligencia artificial ¿una herramienta de doble filo? Especial referencia a su aplicación en el ámbito de la violencia de género". *Aspectos jurídicos de actualidad en el ámbito del Derecho digital*, 141-164. Tirant lo Blanch.

fonaments teòrics de la IA foren establerts anteriorment per Alan Turing.[41] En l'actualitat, no existeix una definició exacta o unànime del que s'entén per IA, per la seva evolució i tipus que comprèn. Segons l'enteniment majoritari de la doctrina, la IA s'entén com una combinació d'algoritmes plantejats amb el propòsit de crear màquines que presenten les mateixes capacitats que l'ésser humà, elaborats a través de l'ús d'una base de dades que, ordenats de forma comprensible *(Smart data)*, un model matemàtic va usant de forma aleatòria fins a establir patrons de correlació determinista entre ells.[42] També és rellevant la definició d'IA acollida per la Comissió Europea com aquella que s'aplica a sistemes que manifesten un comportament intel·ligent, capaces d'analitzar el seu entorn i passar a l'acció –amb cert grau d'autonomia– amb la finalitat d'assolir objectius específics.[43] Destaquen la IA predictiva i generativa: la primera, es basa a fer pronòstics o prediccions precisos sobre esdeveniments futurs, analitzant dades històriques per identificar patrons i relacions amb la finalitat de realitzar les prediccions;[44] en canvi, la segona es defineix com sistemes d'IA destinats específicament a generar –amb diferents nivells d'autonomia– continguts com text, imatges, àudio o vídeo complexos.[45] Per tant, el que anteriorment requeria un exercici manual amb important inversió de temps ara es genera a través de xarxes generatives adversarials *(generative adversarial networks o GAN)*.[46] El present treball se centra en la IA generativa, ja que entre les possibilitats del seu ús destaquen els *deepfakes*.

2) Els deepfakes: estat de la qüestió.

El ***"deepfake"*** (traduït com ultrafals), és un terme compost per la paraula *deep* –provinent de *Deep learning* o aprenentatge profund– i *fake* –fals en anglès–.[47] Aquest terme té origen el

[41] Bello, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI*, 219-248. Colex.
[42] López, S. (2023). "Inteligencia artificial ¿una herramienta de doble filo? Especial referencia a su aplicación en el ámbito de la violencia de género". *Aspectos jurídicos de actualidad en el ámbito del Derecho digital*, 141-164. Tirant lo Blanch.
[43] Comisión Europea (2018). Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan coordinado sobre la inteligencia artificial. COM(2018) 795 final.
[44] González, L. (2023) *Comprendiendo la asombrosa IA: Una guía definitiva para entender la inteligencia artificial.* Aprende IA.
[45] Parlamento Europeo. Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)) 14 de junio de 2023. Consultat a: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.pdf (data de consulta: 1/05/2024)
[46] Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret*, 493-515.
[47] *Ídem*.

2017 a Reddit, quan un usuari anomenat "*deepfake*" va publicar vídeos manipulats i va compartir el codi de programació que habilitava a altres a seguir el seu exemple; els primers vídeos contenien contingut pornogràfic.[48] Els *deepfakes* són producte de la manipulació de material multimèdia preexistent o generats a través de tècniques de *machine learning*, amb l'objectiu de reemplaçar persones simulant que són reals; així, mostren de forma convincent a persones que existeixen, han existit o mai varen existir, fent i/o dient coses que mai van fer i/o dir.[49] Per aprofundir en el binomi *deepfake*-violència masclista és necessari puntualitzar els principals factors d'aquesta connexió: en primer lloc, el sistema cisheteropatriarcal que situa les dones com cossos inanimats i llegeix la seva corporalitat com a objecte de consum; en segon lloc, l'estat denominat per Westerlund com "infoapocalipsi", pel qual no és possible distingir el que és real del que no ho és, fent que la identitat i conducta d'una dona pugui ser manipulada amb certa facilitat i impunitat derivada de la dificultat d'identificar la falsedat i d'haver de combatre la incertesa i la confusió que aquestes produccions sintètiques generen; finalment, l'engany com a nucli dels *deepfakes*, entès com la intencionalitat de faltar a la veritat amb coneixement de la falsedat i com a fórmula de manipulació.[50]

Malgrat que no es pot dir que no existís aquesta tècnica amb caràcter previ al desenvolupament de la IA, sí que es pot concretar que s'ha facilitat, agilitzat i estès la seva pràctica gràcies a aquests tipus de sistemes. La combinació d'aquesta tecnologia amb els avantatges de l'actuació al ciberespai poden perseguir múltiples finalitats malicioses com: destruir la imatge i la credibilitat individual, assetjar o humiliar persones en línia, perpetrar l'extorsió i frau, falsificar documents d'identitat, suplantar identitats en línia, falsificar i manipular proves electròniques, distribuir desinformació, incitar a la violència, odi o altres missatges extremistes o terroristes, interrompre mercats financers o altres conseqüències que provoquin enfrontaments entre diferents Estats.[51] Una altra de les finalitats dels *deepfakes* és la falsificació de proves creades amb *deepfake* o bé presentades com a proves legítimes o bé per viciar les declaracions de testimonis[52]; també per forçar el desistiment de les denunciants

[48] European Parliamentary Research Service (EPRS) (2021) *Tackling deepfakes in European policy.* European Parliament. DOI: 10.2861/325063

[49] González, I. (2023). "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes". *IUS ET SCIENTIA*, 9(2), 157-180.

[50] Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret*, 493-515.

[51] González, I. (2023). "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes". *IUS ET SCIENTIA*, 9(2), 157-180.

[52] Bello, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI*, 219-248. Colex.

o posar en dubte les seves versions. Un altre dels seus objectius seria la creació de conductes fictícies tipificades com a delicte en el Codi Penal que involucren a la víctima i maltractador –conegut com a tàctica de les denúncies creuades– per la iniciació d'un procés penal o inclús la cerca d'aïllament de la víctima, generant una dependència i subordinació més forta respecte del maltractador. Finalment, també es troba la suplantació per part dels maltractadors tant la seva pròpia imatge –enganant les víctimes fent-se passar per amistats o coneguts per acordar una trobada digital o presencial i exercir assetjament *online* o violència física/psicològica– o reemplaçant la identitat de les dones –creant perfils o espais falsos en què la víctima comparteix vídeos íntims o fa demandes o ofertes sexuals explícites–.[53]

S'ha de tenir en compte que els gèneres formals del *deepfake* emergeixen, es renoven i evolucionen ràpidament i sorgeixen altres termes com: *shallowfakes, cheapfakes, fake news, fake nudes, deepnude, face replacement, face-swap, faceshift, voice cloning, deep voice, animoji, pinscreen…*[54] En concret, els ***deepnudes*** o ***"deepfake pornography"***, són producte d'algoritmes d'IA altament sofisticats, capaços d'analitzar i aprendre com hauria de lluir una persona nua –inclús si la imatge d'origen no ho és–. Llavors, la seva creació implica prendre una fotografia d'una persona vestida i, mitjançant l'aplicació d'algoritmes de processament d'imatges i aprenentatge automàtic, transformar-la en una imatge hiperrealista que pareix mostrar aquesta persona nua –amb una elevada precisió per simular detalls com textura de la pell o la il·luminació–. L'alarmant radica en la capacitat d'aquesta tecnologia per enganar a simple vista, ja que les imatges resultants són virtualment indistingibles de les reals; això la fa una eina poderosa i potenciament perjudicial, podent-se emprar aquestes imatges per difamar, assetjar, fer xantatge o danyar la reputació de persones innocents.[55]

3) Impacte dels deepfakes en la societat actual: estadístiques i casos mediàtics.

Segons l'informe *"State of deepfakes 2023"* realitzat per Home Security Heroes, el 98% dels vídeos *deepfake* són pornogràfics, front un 2% que no ho són. El gènere juga un rol important en la selecció de persones per la manipulació del contingut *deepfake*: entre el 98% de

[53] Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret*, 493-515.
[54] Bañuelos, J. (2020). Deepfake: la imagen en tiempos de la posverdad. *Revista Panamericana de Comunicación,* 2(1), 51-61.
[55] Fierro, D. (2023) "La necesidad de sancionar penalmente la difusión de ciertas imágenes creadas con inteligencia artificial." *Diario LA LEY*, Nº 77, Sección Ciberderecho, 3 de Noviembre de 2023, LA LEY.

deepfakes pornogràfics, el 99% del contingut és protagonitzat per dones[56]; en canvi, quan aquests no tenen contingut pornogràfic, els protagonistes són majoritàriament els homes.[57] Aquest fet no ve donat perquè sigui més fàcil crear imatges de dones que d'homes, sinó que depèn de l'orientació que tenen aquests serveis o a qui es vol cridar l'atenció, ja que els grans consumidors de pornografia són els homes.[58]

Les dades d'aquest informe indiquen que entre 2022 i 2023 la quantitat de pornografia *deepfake* creada va augmentar un 464% –un augment de 550% respecte del 2019– passant de 3.725 vídeos el 2022 a 21.019 el 2023. Es tracten de xifres alarmants, perquè 7 de cada 10 pàgines pornogràfiques contenen *deepfakes* i els llocs web amb pornografia *deepfake* tenen una quota de mercat del 90% –manifestant-se així una clara visió de l'ampli consum i difusió del material pornogràfic generat per *deepfake*–. Sobresurt que el 94% de les víctimes treballen en la indústria de l'entreteniment, pel fet que la gran visibilitat les converteix en objectius més probables per ser fàcilment reconegudes i la disponibilitat d'un ampli material visual i auditiu protagonitzat per elles. Aproximadament, existeixen 15 llocs web i fòrums de comunitats de creació de *deepfakes* amb més de 609.464 membres –una part important d'aquestes comunitats i fòrums de creació de *deepfake* es troben en plataformes associades principalment per contingut pornogràfic *deepfake*– i 42 eines *deepfake* fàcils d'utilitzar amb aproximadament 10 milions de cerques mensuals –una de cada tres eines *deepfake* permet als usuaris crear pornografia *deepfake*–. Gràcies a tot l'esmentat amb anterioritat, avui en dia és possible crear gratuïtament i en menys de 25 minuts un vídeo pornogràfic *deepfake* de 60 segons de qualsevol persona fent servir només una imatge clara del seu rostre.

Cal fer esment de l'enquesta realitzada a 1.522 homes estatunidencs sobre pornografia *deepfake* a través d'aquest mateix informe: el 48% d'aquests havien visualitzat pornografia *deepfake* almenys un cop, impulsats majoritàriament per la curiositat tecnològica, seguit per l'atracció de les celebritats i la realització de fantasies; el 74% dels usuaris de pornografia *deepfake* no se senten culpables per fer-ho, sobretot perquè saben que no és la persona real, pensen que no fa mal a ningú o creuen que és una versió més real de la imaginació sexual; a més, un de cada cinc usuaris diaris de pornografia ha canviat la pornografia tradicional per pornografia *deepfake;* destaca que el 20% dels enquestats ha contemplat aprendre a crear

[56] Home Security Heroes (s.d.) *State of Deepfakes 2023. Realities, Threats, and Impact.* Home Security Heroes.
[57] Aider, H., Patrini, G., Cavalli, F., Cullen, L., (Deeptrace Labs). (2019). The State of Deepfakes: *Landscape, Threats, and Impact.*
[58] Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.

pornografia *deepfake* i un de cada deu va admetre haver-ho intentat fer; no obstant això, el 73% dels participants voldria denunciar a les autoritats si algú proper a ells en fos víctima.[59]

En última instància, cal remarcar que, tot i estar front un contingut *fake,* l'impacte psicològic per les víctimes és real i molt elevat, pel fet que el patriarcat és un sistema que penalitza la llibertat sexual de les dones i quan aquesta queda exposada –tot i amb imatges falses– la sensació de desprotecció, violència i pèrdua de control és real, equiparant-se les seves conseqüències a les de qualsevol mena de ciberviolència masclista. La ciberviolència masclista afecta directament la salut mental de les víctimes amb conseqüències com la pèrdua de qualitat de vida de les dones, l'impacte en la seva situació laboral per no poder participar en igualtat de condicions en el món digital o l'atenció mèdica que requereixen, amb elevades taxes d'ansietat, depressió, autolesions i suïcidi.

En quant els casos de *deepfake* a Espanya, cal remarcar que tot i l'existència de casos disseminats arreu de l'Estat, es tracta d'un fenomen molt recent, per la qual cosa les investigacions i procediments encara resten oberts –per la complexitat de la matèria, falta de coneixements i recursos i manca de regulació–. Malgrat això, alguns casos sí que han rebut sentència, tot i que sembla que aquestes no s'han fet públiques encara a les bases de dades jurídiques. Per això, s'analitzaran alguns dels casos mediàtics que s'han donat a Espanya.

El cas amb més ressò mediàtic ha estat el "cas Almendralejo", a Badajoz, pel fet que es van crear *deepfakes* –en la seva modalitat de *deepnude*– de vint-i-dues menors d'edat realitzats també per menors –algun d'ells inclús menor de catorze anys i, per tant, inimputable–. Aquests, tenien un grup de WhatsApp on difonien les imatges de les seves companyes de classe "despullades" a través d'IA.[60] Els menors entre catorze i divuit anys es podrien enfrontar a penes amb finalitat educativa –no sancionadora– i sense internament en règim tancat, ja que seria una pena menys greu –podent ser, per tant, una llibertat vigilada i l'obligació d'assistir tallers o formació, treballs en benefici de la comunitat o allunyament de les víctimes–.[61] Actualment, les famílies de les víctimes estudien la proposta de la Fiscalia de Menors per arribar a un acord de conformitat amb les parts: es contempla la condemna d'un any de llibertat vigilada aparellada de l'obligació de fer cursos de formació relacionats amb el

[59] Home Security Heroes (s.d.) *State of Deepfakes 2023. Realities, Threats, and Impact.* Home Security Heroes.
[60] Apolo, C. (2023) Lo que se sabe hasta el momento del caso de los falsos desnudos de las menores en Almendralejo (Badajoz). *elEeconomista.es*
[61] Público. (2023). La app de falsos desnudos no tiene responsabilidad penal, pero podría ser acusada de negligencia. *Público*.

bon ús de les tecnologies, educació afectivosexual i igualtat de gènere.[62] Els delictes pels quals podrien ser condemnats en cas d'arribar a la sentència de conformitat serien el de pornografia infantil i el d'integritat moral.[63]

A Pamplona, un jove de divuit anys fou condemnat com a autor d'un delicte de coaccions i contra la integritat moral per difondre imatges de dues companyes d'institut les quals mostrava nues a través d'IA. El Jutjat d'Instrucció núm. 4 de Pamplona va assumir la investigació i es va fer un judici ràpid en què l'investigat va assumir els fets, essent condemnat a un any de presó i una ordre d'allunyament de les dues víctimes, la prohibició de comunicació de dos anys i sis mesos i una indemnització de 1.500 euros per cada víctima.[64]

A Utebo, Saragossa, el febrer de 2024 es va destapar un cas de manipulació d'imatges amb IA per crear *deepnudes*, afectant cinc menors d'entre catorze i quinze anys. Es van obrir diligències penals a set menors com a presumptes autors de delicte de pornografia infantil i contra la integritat moral –tot i que hauria sis presumptament implicats més, inimputables per ser menors de catorze anys–. No obstant això, en el cas dels inimputables penalment, si la causa arriba a judici i es dicta sentència condemnatòria, els seus pares podrien ser obligats a fer-se càrrec de les possibles indemnitzacions a les víctimes.[65]

Si bé els casos de *deepfakes* ocorreguts a l'Estat espanyol estan començant a ser sancionats, s'observen discrepàncies a l'hora de determinar en quins delictes s'han de subsumir tals conductes. Arran d'aquest fet, es plantegen una sèrie d'incògnites a les quals s'intentarà donar resposta al llarg del treball: És politicocriminalment adequada la sanció d'aquestes conductes com un delicte de coaccions? És necessària una reforma que unifiqui els criteris respecte de la seva qualificació jurídica? Quin és el tipus delictiu que millor s'adequa a aquestes conductes?

4) Transformació de la ciberviolència masclista a través dels deepfakes: perspectives des de la teoria del delicte.

En el que respecta a la IA generativa destaquen canvis i adaptacions en els *modus operandi* de determinats tipus delictius, ja que la IA es presenta com una oportunitat pels

[62] Moral, G. (2024). Un acuerdo podría evitar el juicio por el caso de los falsos desnudos por IA en Almendralejo. *el Periódico Extremadura.*
[63] EFE. (2024). Las víctimas de los falsos desnudos de Almendralejo estudian propuesta de acuerdo de la Fiscalía. *EFE*.
[64] Público (2024). Condenan a un joven de 18 años por difundir imágenes falsas de compañeras desnudas generadas por IA. *Público.*
[65] Coloma, M. A. (2024). Caso de las fotos trucadas con IA en Utebo: las víctimas de los falsos desnudos son 5 chicas. *Heraldo.*

ciberdelinqüents: milloren els atacs, obtenen més beneficis en menys temps, accedeixen a noves víctimes, creen mitjans d'atac més innovadors, reforcen el seu anonimat i poden fer ús d'aquests sistemes amb pocs coneixements tècnics. Les característiques més rellevants de la IA generativa per la comissió de ciberviolència masclista són: la utilitat de models de llenguatge generatiu per suplantar la identitat i capacitat d'aquests models per afavorir que els ciberdelinqüents es guanyin la confiança de les víctimes, l'ús de *deepfakes* basats en imatges, vídeos o àudio i la possible combinació de diferents tècniques d'IA generativa buscant major efectivitat, entre altres. Tal com s'ha indicat anteriorment, no es tracta de l'aparició de nous delictes, sinó d'eines que agilitzen i promouen la seva pràctica, ja que el principal avantatge de la IA generativa és facilitar i millorar la qualitat del material audiovisual.[66]

En el cas concret dels *deepfakes*, es tracta d'una nova forma d'exercir violència per mitjans digitals que amplien el seu abast i magnifiquen les conseqüències de les víctimes[67] La transformació més impactant que han tingut els *deepfakes* sobre la ciberviolència masclista recau sobre l'autoria d'aquests tipus de conducta. Per una banda, destaca l'elaboració anònima que ofereixen les eines d'IA generativa, les quals poden obstaculitzar l'actuació de les autoritats competents: un dels principals objectius després de la detecció d'un fet delictiu és identificar els responsables –afavorint així la repressió del delicte i reparació del dany–, qüestió amb dificultats significatives des de l'aparició d'Internet i que es veu agreujada amb l'ús de la IA.[68] En el cas dels *deepnudes,* la naturalesa anònima i elusiva d'Internet fan que rastrejar i atribuir responsabilitats en la creació i distribució d'aquestes imatges sigui una tasca difícil pel fet que els perpetradors se solen ocultar darrere capes d'anonimat i tecnologia –dificultant la identificació i persecució dels responsables–; aquest és un problema crucial en la lluita contra aquesta forma d'abús digital perquè la falta de rendició de comptes permet que aquestes pràctiques continuïn proliferant.[69] Per altra banda, es possibilita que persones sense coneixements especialitzats puguin crear contingut fictici pel propòsit que considerin, podent constituir l'exercici de la violència contra les dones un d'aquests.[70]

---

[66] González, I. (2023). "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes". *IUS ET SCIENTIA*, 9(2), 157-180.
[67] Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.
[68] González, I. (2023). "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes". *IUS ET SCIENTIA*, 9(2), 157-180.
[69] Fierro, D. (2023) "La necesidad de sancionar penalmente la difusión de ciertas imágenes creadas con inteligencia artificial." *Diario LA LEY*, Nº 77, Sección Ciberderecho, 3 de Noviembre de 2023, LA LEY.
[70] Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret*, 493-515.

L'anteriorment esmentat fa que en un context viral com l'actual –on les imatges circulen molt de pressa–, la capacitat de resposta sigui ínfima respecte del dany causat. La dificultat de control d'aquestes tecnologies de generació d'imatge es complica per la facilitat d'accés que hi ha i les dificultats per realitzar una traçabilitat de la imatge.[71] Tenint en compte que els *deepfakes* són tant un fenomen tecnològic com cultural, legal o ètic, front un abordatge parcial i incomplet que impedeix conjugar tots els elements que componen aquesta nova realitat es proposa un sistema de triple resposta des de l'àmbit jurídic –amb especial atenció als problemes de prova i tipificació penal–, polític –en relació amb la incertesa informativa en l'etapa de la postveritat–, i tècnic –vinculat a la capacitat de dissenyar altres sistemes GAN de detecció de *deepfakes*.[72]

De l'anterior es desprèn com la doctrina ha abordat els reptes que suposen les variacions en la comissió delictiva de la ciberviolència masclista a través dels *deepfakes*. Malgrat això, a continuació es posen de manifest altres qüestions a considerar, ja que es tracta d'un àmbit molt recent i en constant evolució, el qual requereix un tractament amb profunditat que s'ha d'anar actualitzant.

En relació amb l'autoria dels *deepfakes,* també cal demanar-se des d'una perspectiva del Dret penal qui seria imputable subjectivament i fins a quin punt arriba la responsabilitat penal (i civil) dels implicats: és responsable el creador del mateix *deepfake* o el creador d'aquesta IA?, es dóna una despersonalització de la responsabilitat a causa de l'autonomia de la IA? El Reglament de la IA no aporta una resposta clara respecte de la IA de risc limitat[73] –en la qual s'inclouen els *deepfakes–,* perquè no aporta mecanismes punibles sinó que simplement indica que els proveïdors i responsables del desplegament han de complir amb determinades obligacions de transparència per garantir que els usuaris finals són conscients que estan interactuant amb una IA[74] –a diferència del que passa amb els sistemes d'alt risc, la responsabilitat dels quals sí que es troba regulada–. Respecte de l'autonomia de la IA, Eloy

[71] Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.
[72] Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret*, 493-515.
[73] Comisión Europea (2024) *Ley de IA.* https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai
Noció d'IA de "risc limitat": el risc limitat es redueix als riscos associats amb la manca de transparència en l'ús de la IA. La Llei d'IA introdueix obligacions específiques de transparència per garantir que els éssers humans estiguin informats quan calgui, fomentant la confiança. Els proveïdors també hauran d'assegurar-se que el contingut generat per IA sigui identificable. A més, el text generat per IA publicat amb el propòsit d'informar el públic sobre assumptes d'interès públic s'ha d'etiquetar com a generat artificialment. Això també s'aplica al contingut d'àudio i de vídeo que constitueix falsificacions profundes (*deepfakes*).
[74] EU Artificial Intelligence Act (2024). *Resumen de alto nivel de la Ley AI.* https://artificialintelligenceact.eu/es/high-level-summary/

Velasco –magistrat de la Sala de lo Penal de l'Audiència Nacional– indica que l'ús que es faci de la IA depèn de l'ésser humà, no podent-se culpar a la màquina dels delictes comesos, ja que no tenen sentiment de culpa, no entenen, ni tenen empatia o reprotxabilitat.[75]

Endemés, cal destacar que els *deepfakes*, vulneren 2 grans drets: la protecció de dades o la privacitat –perquè es difon informació que, tot i ser essencialment falsa, utilitza dades personals reals com el rostre o la veu sense consentiment de l'afectat–; d'altra banda, la intimitat, honor i pròpia imatge –ja que la informació sol estar relacionada amb la vida íntima o sexual de la persona afectada–.[76] En relació amb aquest fet, sorgeix una altra innovació problemàtica que comporten els *deepfakes*: el seu hiperrealisme. Això dificulta la tasca de les autoritats per tipificar la conducta, perquè per exemple en els *deepnudes* –on l'hiperrealisme és de cada cop més latent– és complex tipificar una conducta com un delicte contra l'honor, la intimitat o la integritat moral quan aquell cos nu no correspon realment a la persona afectada. No obstant això, a causa d'aquest hiperrealisme, per molt que la informació pugui ser falsa, les dades personals –com la cara de la víctima– sí que són reals, la qual cosa indueix a confusió fins al punt de no poder determinar si aquell contingut és real o fictici, incidint directament a la vida íntima o sexual de l'afectada.

5) Marc regulador dels deepfakes: regulació a escala europea i a escala nacional.

A escala europea, destaca la regulació a través del Reglament Europeu d'Intel·ligència Artificial, recentment aprovat el 13 de març de 2024. Es tracta del primer marc jurídic integral sobre la IA en tot el món, el qual aborda els riscos de la IA i posiciona Europa per desenvolupar un paper de lideratge a escala mundial. Aquest, segueix un enfocament basat en el risc, establint-se quatre nivells de risc per als sistemes d'IA –risc inacceptable, alt risc, risc limitat i risc mínim o nul–, determinant-se quines són les conductes que es troben inserides dins cada categoria i les obligacions que hauran de complir els sistemes d'IA en funció del nivell de risc que impliquin.[77] L'objectiu de les seves normes és fomentar una IA fiable a Europa i fora d'aquesta, que respecti els drets fonamentals, la seguretat i els principis ètics, abordant els riscos de models d'IA molt potents i impactants. Entre les normes proposades destaquen: abordar els riscos creats específicament per les aplicacions d'IA, prohibir les pràctiques d'IA que plantegen riscos inacceptables, definir obligacions específiques dels

[75] Valdés, B. (2024) Fiscal Elvira Tejada, sobre el uso de IA para simular la identidad: «No tiene una respuesta adecuada en el Código Penal». *Confilegal.*
[76]Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.
[77] Comisión Europea (2024) *Ley de IA*. https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai

responsables del desplegament[78] (o implementadors/usuaris) i proveïdors (o desenvolupadors) d'aplicacions d'IA d'alt risc, exigir una avaluació de conformitat abans de la posada en servei o introducció en el mercat d'un determinat sistema d'IA, posar en marxa l'execució després de la introducció en el mercat d'un determinat sistema d'IA i establir una estructura de governança en l'àmbit europeu i nacional.[79]

En particular, es precisa la definició dels *deepfakes* (ultrafalsificació) en l'art. 3.60) com contingut d'imatge, àudio o vídeo generat o manipulat per una IA que s'assembla a persones, objectes, llocs o altres entitats o esdeveniments existents que pot induir a una persona a pensar erròniament que són autèntics o verídics.

A més, l'art. 50.4 sobre les obligacions de transparència pels proveïdors i usuaris de determinants sistemes d'IA, indica que els responsables del desplegament d'un sistema d'IA que generi o manipuli continguts d'imatge, àudio o vídeo que constitueixin un *deepfake*, hauran de revelar que el contingut ha estat generat o manipulat artificialment; aquesta obligació no s'aplicarà quan l'ús estigui autoritzat per la llei per detectar, prevenir, investigar o enjudiciar infraccions penals. Quan el contingut formi part d'una obra o programa manifestament artístic, creatiu, satíric o de ficció, les obligacions de transparència establertes en aquest apartat es limiten a l'obligació de fer pública l'existència d'aquest contingut generat o manipulat artificialment d'una manera adequada que no dificulti l'exhibició o el gaudi de l'obra. Els responsables del desplegament d'un sistema d'IA que generi o manipuli un text publicat per informar el públic sobre qüestions d'interès públic, han de revelar que el text ha estat generat o manipulat artificialment; aquesta obligació tampoc no s'aplicarà quan l'ús estigui autoritzat per llei per detectar, prevenir, investigar o enjudiciar infraccions penals o quan el contingut generat per IA hagi estat sotmès a un procés de revisió humana o de control editorial i quan una persona física o jurídica tingui la responsabilitat editorial per la publicació del contingut. En el mateix sentit, es pronuncia l'atès 134, tot i que indicant que el compliment d'aquesta obligació de transparència no s'ha d'interpretar com un indicador que l'ús del sistema o de la seva informació de sortida obstaculitzin el dret a la llibertat d'expressió i el dret de la llibertat de les arts i ciències garantits a la Carta –concretament quan el contingut formi part d'una obra o programa manifestament creatius, satírics, artístics o de ficció, subjectes a les garanties adequades pels drets i llibertats de tercers. En aquests casos, l'obligació de transparència dels *deepfakes* es limita a la divulgació de l'existència

[78] Reglamento de Inteligencia Artificial. Noció de "responsable del desplegament": una persona física o jurídica o autoritat, òrgan o organisme d'un altre caràcter públic que utilitzi un sistema de IA sota la seva pròpia autoritat, excepte quan l'ús s'emmarqui en una activitat personal de caràcter no professional.
[79] Comisión Europea (2024) *Ley de IA*. https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai

d'aquests continguts generats o manipulats d'una forma adequada que no obstaculitzi la presentació i gaudi de l'obra –inclosa la seva explotació i ús normals– tot mantenint la utilitat i qualitat de l'obra.[80]

A Espanya, la creació d'imatges sexuals creades per IA o *deepfakes* pornogràfics, no es contempla encara com a delicte específic en el Codi Penal; ara bé, atesa la idea de violència masclista com tota violència que s'exerceix contra les dones, la creació d'aquest tipus d'imatges no deixa de ser una forma de violència més contra elles.[81] El 13 d'octubre de 2023 es va publicar al Butlletí Oficial de les Corts Generals la Proposició de Llei Orgànica de regulació de les simulacions d'imatges i veus de persones generades per mitjà de la intel·ligència artificial, presentada pel Grup Parlamentari Plurinacional Sumar. Aquesta s'articula com a mecanisme per l'ús de tècniques de recreació d'imatge i veu mitjançant IA –conegut com a *deepfake*– a l'empara del dret fonamental a la llibertat d'expressió mentre s'esbossa un marc regulador per assegurar la resta de drets fonamentals previstos en el nostre ordenament jurídic –en especial el dret a l'honor, intimitat i pròpia imatge–.

Entre les fonts citades a la Proposta es troben: les "Conclusions relatives al Pla Coordinat sobre la IA" (2019) del Consell Europeu, les conclusions sobre la "Carta dels Drets Fonamentals en el context de la IA i canvi digital de la Presidència del Consell de la Unió Europea" (2020), el "Llibre Blanc de la UE sobre la IA" (2020), la "Proposta de Reglament Europeu pel qual s'estableixen normes harmonitzades en matèria d'IA" (2021) instada per la Comissió Europea, l'estudi *"Tackling deepfakes in European policy"* del Servei d'Estudis del Parlament Europeu (2021) i el "Reglament de Serveis Digitals" del Parlament Europeu.[82]

Aquesta preveu diverses modificacions legislatives: en primer lloc, la Modificació de la Llei 13/2022, de 7 de juliol, General de Comunicació Audiovisual (art. 1) incorporant com infracció molt greu en l'art. 157 la difusió d'imatges, vídeos o audios *deepfake* sense prèvia autorització o consentiment exprés de la persona objecte d'aquests, excepte quan incloguin de forma clara l'advertència de la seva condició d'imatge o soroll generats per IA; com a excepció, es determina que no es troba dins aquestes infraccions l'ús d'imatges o àudios *deepfake* autoritzats per llei per detectar, prevenir, investigar i perseguir infraccions penals o

[80]Reglamento de Inteligencia Artificial. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

[81] Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.

[82] Oyarzábal, N. i Pérez, R. (2023) *Deepfake vs. Derecho al honor, intimidad y propia imagen.* Cuatrecasas.

quan el contingut formi part d'una obra o programa evidentment creatiu, satíric, artístic o de ficció. La Modificació de la Llei Orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge (art. 2) considera com intromissió il·legítima la difusió i ús d'imatges, vídeos o àudios *deepfake* sense prèvia autorització o consentiment exprés de l'afectat, excepte que incloguin de forma clara i excel·lent un advertiment de la seva condició d'imatge o àudio generat artificialment per IA; l'advertiment haurà de figurar sobreimprès i llegible a la imatge i pel cas dels àudios caldrà fer una advertència audible abans i després de la difusió. A la Modificació de la Llei Orgànica 10/1995, de 23 de novembre, del Codi Penal (art. 3) es preveu la creació d'un nou art. 208 bis CP, considerant com injúria l'acció que sense autorització i amb ànim de menyscabar l'honor, fama, dignitat o pròpia estima d'una persona, recrei mitjançant tecnologia *deepfake* per la pública difusió de la imatge corporal o àudio; a més, es modifica l'art 211 CP afegint un segon paràgraf el qual indica que la difusió d'aquests a les xarxes socials seran considerats com injúries fetes amb publicitat. Es modifica la Llei 1/2002, de 7 de gener, d'Enjudiciament Civil (art. 4) incloent en l'art. 727 una mesura cautelar de retirada de les simulacions d'imatges, vídeos o veus, generades per sistemes automatitzats, programari, algorismes o mecanismes intel·ligència artificial a petició de la persona afectada o els seus representants. La Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (art. 5) determina en l'art. 22 bis l'aplicació de la present llei a les dades personals generades per IA que siguin difosos públicament. S'inclou, a més, la modificació de la Llei 3/1991, de 10 de gener, de Competència Deslleial (art. 6) respecte dels actes d'engany, considerant-se deslleial l'ús en comunicacions comercials d'imatges o sorolls *deepfake* o la modificació de les aparences corporals usats en tals comunicacions per sistemes de processament d'imatges sense advertir-ho en la comunicació comercial de forma clara. En l'art. 7 es proposa la Modificació de la Llei Orgànica 5/1985, de 19 de juliol, del Règim Electoral General afegint un nou art. 144 bis que inclogui els delictes de distribució maliciosa d'imatges i veus generades per IA. En la disposició addicional primera es proposa la creació del Consell de Participació Ciutadana per la supervisió i avaluació de la IA, establint la seva composició, objecte i desenvolupament de la normativa precisa; la disposició addicional segona suggereix la creació del Consell Consultiu sobre l'ús de la IA pel desenvolupament normatiu i reglamentari de les iniciatives legislatives necessàries per la protecció dels drets

fonamentals i llibertats públiques; en aquesta disposició també es regula la seva composició, funcions i desenvolupament de la normativa precisa.[83]

És important tenir en compte que la recent aprovació del Reglament Europeu d'Intel·ligència Artificial definirà el marc d'actuació i, per tant, la Proposició de Llei espanyola s'hauria d'adequar al disposat per la normativa europea, perquè l'harmonització legal internacional és molt important per evitar la impunitat de les actuacions il·legals des de fora d'Espanya.[84]

Malgrat la visible manca d'una regulació harmoniosa i específica sobre els *deepfakes* a Espanya, les víctimes de *deepfakes* pornogràfics a l'Estat espanyol poden acudir directament al canal prioritari de l'Agència Espanyola de Protecció de Dades –canal indicat per situacions en què existeixi sensibilitat, sigui per qüestions sexuals o en compartició d'imatges íntimes o bé on es vegin agressions en temes d'assetjament, fonamentalment escolar–; en menys de 24 hores s'intentarà evitar que es comparteixi aquesta informació o es continuï difonent aquesta per tallar la cadena de transmissió. Així mateix, també es pot accedir a la via civil a través d'una compensació econòmica per danys i perjudicis quan s'hagin patit danys quantificables i reals –molts cops aquests tipus de situacions donen lloc a aquest–. Com a darrera opció es pot activar la via penal, pel fet que compartir o difondre imatges pornogràfiques –creades o no amb IA– comporta la comissió d'un delicte tipificat en el CP –es tracti de menors o no–.[85] És a dir, es tracta d'uns actes que poden suposar un risc penalment rellevant que es podria subsumir en algun dels tipus previstos actualment al CP; no obstant això –com s'ha anat apuntant i com es detalla específicament en el següent apartat–, aquesta via encara requereix algunes modificacions que realment la facin viable per assolir una resposta politicocriminalment satisfactòria envers un problema de tal magnitud.

4- PROPOSTES

1) Propostes de lege ferenda per la penalització dels deepfakes.

L'aparició de la IA ha comportat un abans i un després en la justícia a escala global i és per això que els diversos països arreu del món estan concentrant els seus esforços en com tractar

[83] Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial. Boletín Oficial de las Cortes Generales, Núm 23-1, de 13 de octubre de 2023.
[84] Ansón, R. (2023) *Deepfake y Legislación: retos y proposición de Ley Orgánica.* Bufete Mas y Calvet.
[85] Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.

aquesta matèria judicialment. Com s'ha detallat anteriorment, la Unió Europea ha aprovat recentment el Reglament d'IA i els Estats Membres estan donant les primeres passes per la seva regulació, com bé seria el cas italià –amb l'aprovació pel Consell de Ministres el 23 d'abril de 2024 d'un Decret que castiga els *deepfakes* a través d'un delicte específic, amb pena de presó d'un a cinc anys per la difusió de vídeos o imatges alterades amb IA sense consentiment, causant dany injust–[86] o el cas espanyol –amb la Proposició de Llei Orgànica de regulació de les simulacions d'imatges i veus de persones generades per mitjà de la intel·ligència artificial–. Malgrat això, en l'àmbit nacional espanyol –tot i la recent proposta– encara no s'ha adoptat una regulació específica. Davant les controvèrsies de la doctrina i la inexistència d'un marc regulador, es procedeix a plasmar una proposta de *lege ferenda* per la penalització dels *deepfakes* a Espanya.

Abans d'entrar en el debat doctrinal, es determina la necessitat d'una harmonització de les regulacions existents sobre violència de gènere, violència sexual i ciberviolència masclista, amb la consegüent harmonització de les reformes des del 2004 –amb la LOMPIVG–, passant per la Llei Orgànica 10/2022, de 6 de setembre, de garantia integral de la llibertat sexual, fins al recent anunci l'abril del 2024 del Ministeri de Justícia respecte d'una nova Llei Orgànica per reforçar la protecció a les víctimes de violència de gènere i el seu dret d'accés a la justícia. Val a dir que per aquesta cohesió s'hauran d'incloure les pertinents referències a la IA, les quals a hores d'ara són inexistents.

Com s'ha esmentat, la doctrina jurídica espanyola està dividida pel que fa a la regulació dels *deepfakes*. D'una banda, n'hi ha que consideren essencial la creació d'un tipus penal específic pels *deepfakes* –tal com s'argumenta a continuació–; d'altres, consideren que això no és necessari i aposten per fer modificacions en els tipus penals existents. D'altra banda, n'hi ha que creuen que en cas de penalitzar-se*,* aquests s'haurien de tractar com a delictes contra l'honor, tot i que n'hi ha alguns que consideren més adequat inserir els *deepfakes* en els delictes contra la integritat moral –essent aquesta la visió que es proposa en el treball–.

Quant a la primera de les discussions, en el present treball s'opta per la creació d'un tipus penal específic que castigui aquells que creïn o difonguin *deepfakes*. Aquesta és una idea que sosté la Proposició de Llei Orgànica de regulació de les simulacions d'imatges i veus de

[86] Sorrentino, C. (2024) *Intelligenza artificiale: cosa prevede la normativa italiana.* Osservatori.net.

persones generades per mitjà de la intel·ligència artificial –tot i que considerant crear un nou tipus d'injúria–. Segons Diego Fierro, lletrat de l'Administració de Justícia, la regulació d'aquesta matèria no pot tenir un enfocament estàtic o rígid, sinó que –tenint en compte la ràpida evolució de la IA– les lleis i regulacions en aquest àmbit han de ser adaptables i flexibles perquè aquestes no quedin obsoletes ràpidament. A més, Fierro també apunta que la inclusió de delictes específics relacionats amb la IA en el CP pot ser una mesura necessària en alguns casos per garantir que les conductes delictives associades amb aquesta tecnologia siguin adequadament sancionades; en concret, creu que podria ser de gran utilitat sancionar penalment l'elaboració de certes imatges creades amb IA –els *deepfakes*– amb un tipus penal especial.[87] Com a darrer incís, es considera necessària l'existència d'aquest tipus específic perquè tot allò que manca de tipificació no consta i, per tant, és com si no existís, pel fet que no permet la seva correcta detecció ni comptabilització –donant lloc a una elevada xifra negra del delicte–, dificultant-se així la seva sanció.

Un cop establerta la necessitat de crear un tipus penal específic pels *deepfakes* sorgeix la segona de les incògnites: quina és la millor forma per tipificar-lo? Com a qüestió prèvia, cal negar la cabuda dels *deepfakes* en els delictes de suplantació d'identitat (art. 401 CP) per tractar-se aquest darrer d'un delicte anacrònic a una realitat caracteritzada per la IA. En relació amb això, a la STS 3961/2009 d'1 de juny de 2009 s'exposa una falta de concepte unànime i sense fissures, tot i que la concepció dominant argumenta que *"no basta una suplantació momentània i parcial, sinó que es precisa continuïtat i persistència."* Per tant, tot i que en alguns casos els *deepfakes* es puguin emprar per suplantar la identitat de les víctimes, no es pot dir que es compleixi amb el tipus objectiu consistent en aquesta suplantació continua i persistent; la finalitat darrera dels *deepfakes* no és tal suplantació de la identitat, sinó la creació d'un contingut hiperrealista amb finalitats malicioses –esmentades al llarg del treball– com podrien ser la falsificació de proves, viciar les declaracions de testimonis, incitar a la violència o odi, assetjament i humiliació, destruir la imatge i credibilitat individual, perpetrar l'extorsió i frau, amenaçar i coaccionar a la víctima, entre d'altres.

Entrant en l'incipient debat doctrinal sobre la seva tipificació en el CP, malgrat que alguns especialistes han considerat que es tracta d'un delicte contra l'honor (arts. 208-210 CP) –com també apunta Sumar en la seva Proposició de Llei Orgànica–, en el present treball es considera més adient tipificar els *deepfakes* com un delicte contra la integritat moral

[87] Fierro, D. (2024). *La (in)existente necesidad de regular delitos cometidos con inteligencia artificial.* Economist & Jurist.

(Llibre II, Títol VII del Codi Penal: de les tortures i altres delictes contra la integritat moral). En primer lloc, es considera un error tipificar-ho com a delicte d'injúries dels arts. 208 a 210 CP perquè per molt que amb un *deepfake* es pugui lesionar la dignitat d'una persona, menyscabant la seva fama o atemptant la seva pròpia estima –complint-se així amb el seu tipus objectiu– no es considera recomanable tipificar-ho com a tal, ja que és un delicte privat que necessita querella de l'ofès o dels seus representants –no essent perseguible d'ofici–, la qual cosa dificultaria la seva detecció i posterior sanció. En segon lloc, és primordial i obligatòria la realització –o el seu intent– d'una conciliació prèvia amb la part a la qual es vol denunciar amb anterioritat al procediment judicial, perquè sense presentar certificació d'haver celebrat –o intentat celebrar– aquest acte de conciliació, la querella no serà admesa a tràmit (tal com es deriva de l'art. 804 de la Llei d'Enjudiciament Criminal).[88] En darrer terme, s'ha de tenir en compte que si es castiguen els *deepfakes* com a delicte d'injúries s'estaria trencant la proporcionalitat entre la gravetat de la conducta i la pena, perquè es tracta d'una conducta especialment gravosa per la víctima –en especial en casos de *deepnudes*– la qual si fos castigada per injúries rebria una pena irrisòria en proporció a la seva gravetat –essent aquesta de tres a set mesos i màxim de sis a catorze mesos quan les injúries greus es facin amb publicitat–.

Exposats els motius pels quals no és convenient la regulació com a delicte d'injúries, es procedeix a determinar la seva correcta tipificació com a delicte contra la integritat moral de l'art. 173.1 CP. D'entrada, s'eliminen els obstacles que es donaven en el cas de les injúries, ja que els delictes contra la integritat moral no obliguen a una conciliació prèvia al judici entre querellant i querellat –conciliació que únicament és obligatòria en delictes que atempten contra l'honor–. Respecte de les penes, és perceptible una major proporcionalitat entre la gravetat de la conducta i la pena aparellada, pel fet que l'art. 173.1 CP castiga aquestes conductes amb pena de presó de sis mesos a dos anys. A més, és un tipus penal molt obert, en què en principi tenen cabuda totes les conductes capaces de lesionar aquest bé jurídic, sempre que el mitjà comissiu emprat es pugui reputar com a "tracte degradant" i el menyscapte de la integritat moral mereixi ser considerat com a greu –com bé seria el cas dels *deepfakes,* també en la seva modalitat de *deepnudes*–; endemés, aquesta figura actua com un tipus de recollida de totes aquelles afectacions importants a la integritat moral que no es poden subsumir en altres conductes més greus.[89] Cal remarcar també que la majoria dels

[88]Conceptos jurídicos (2024). *La injuria.* Conceptosjurídicos.com https://www.conceptosjuridicos.com/injuria/
[89] Felip, D. i Ragués, R. (2018). "Torturas y otros delitos contra la integridad moral". Lecciones de Derecho Penal Parte Especial (Sexta Edición), 117-131. Atelier.

delictes de ciberviolència masclista anteriors a l'aparició de la IA comprenen la integritat moral com a bé jurídic a protegir *(remissió al punt 2.4)*, donant-se llavors l'harmonia buscada amb aquesta proposta de les diferents regulacions existents. A més, alguns casos exposats en el punt 3.3 evidencien que les recents condemnes en aquesta matèria han seguit aquesta línia. Establerta la seva pertinent regulació com a delicte contra la integritat moral, es proposa la creació d'un nou apartat dins de l'art. 173.1 CP –sense la necessitat de crear un nou article– pel fet que en aquest ja s'enumeren diverses conductes constitutives de delicte contra la integritat moral, com l'assetjament laboral o immobiliari. Aquest fet dóna lloc al càstig del delicte de *deepfake* en el nou art. 173.1 II CP, amb un redactat similar al següent:

Artículo 173 del Código Penal

1. El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

Igual pena se impondrá a quienes generen sin autorización contenidos de imagen, vídeo, texto o audio manipulados mediante la inteligencia artificial que pudieran inducir a alguien a pensar erróneamente que son auténticos cuando afecten gravemente la integridad moral de quienes aparezcan en estos.

Se impondrán las penas en su mitad superior cuando mediante la inteligencia artificial se manipulen contenidos de tal modo que la persona perjudicada aparezca desnuda, induciendo a alguien a pensar erróneamente que dicho contenido es auténtico. Tal pena también se impondrá cuando el contenido haya sido sometido a especial difusión. También cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección.

Al llarg del treball s'han exposat els problemes sobre l'autoria dels fets i la conseqüent atribució de responsabilitat penal –pel fet que és molt complex saber qui ha estat l'artífex d'un *deepfake,* dificultant-se així la seva perseguibilitat–. En aquest punt, se suggereix que quan l'art. 173.1 CP es refereix a *"el que infligiera a otra persona…"* es consideri la responsabilitat dels titulars dels comptes a les xarxes socials mitjançant els quals es creïn o difonguin els *deepfakes.* Així mateix –en concordança amb línia seguida pel Reglament d'IA respecte de la IA d'alt risc– es planteja la responsabilitat dels propietaris de les plataformes en les quals es difonguin els *deepfakes*, sense oblidar la potencial responsabilitat penal de les mateixes plataformes d'IA.

Cal destacar que tot i la seva regulació com a delicte contra la integritat moral, res impedeix poder castigar els *deepfakes* en concurs real amb altres conductes constitutives de delicte. Per una banda, es podria donar un concurs real amb un delicte de lesions de l'art. 147 CP, per les lesions psíquiques que s'ha manifestat que els *deepfakes* poden provocar a les víctimes –entre elles, elevades taxes d'ansietat, depressió, autolesions i suïcidi–. D'altra, seria possible el

concurs real amb els delictes contra l'honor dels arts. 208 a 210 CP, ja que com s'ha indicat anteriorment, es donen conductes que es relacionen amb els requerits d'aquest tipus penal. Finalment, també es pot considerar el concurs real de delictes amb els delictes contra la llibertat sexual del Títol VIII –entre els quals es troben l'agressió sexual, l'agressió sexual a menors de 16 anys, l'assetjament sexual, l'exhibicionisme, la provocació sexual i els delictes relatius a prostitució, explotació sexual i corrupció de menors–[90] per les relacions dels *deepfakes* amb aquests delictes, ja que aquests es poden emprar per coaccionar a la víctima –major o menor de 16 anys– per mantenir relacions amb l'agressor o per generar pornografia infantil, entre d'altres.

La regulació proposada en l'àmbit penal ha d'anar en concordança amb una regulació en àrees complementàries per assolir un marc legal complet respecte dels *deepfakes*. Aquesta és la línia seguida per la Proposició de Llei Orgànica de regulació de les simulacions d'imatges i veus de persones generades per mitjà de la intel·ligència artificial, pel fet que proposa la modificació de diverses lleis *(remissió al punt 3.5)*, tot i que també es consideren necessàries les modificacions en la regulació en l'àmbit de la propietat intel·lectual, la responsabilitat civil per danys, respecte de les qüestions ètiques i de drets humans relacionats amb el seu ús i desenvolupament, la promoció de transparència i rendició de comptes en l'ús i desenvolupament de sistemes d'IA. A més, com els delictes relacionats amb la IA poden anar més enllà de les fronteres nacionals, la cooperació internacional és crucial per abordar el problema de forma efectiva.[91]

A tall de reflexió, tot i la latent necessitat de regular aquesta conducta, es recomana dur a terme plans de prevenció i campanyes de sensibilització en l'àmbit nacional i internacional per crear consciència de les implicacions psicològiques, ètico-morals i legals que implica la creació d'aquests *deepfakes* i intentar així que els delictes en aquest àmbit disminueixin.

2) Propostes de preparació dels jutges i fiscals enfront dels casos de deepfakes.

Es pot percebre la IA com una arma de doble tall: o bé com un avanç en la verificació del material probatori i audiovisual, o bé com una eina per obstaculitzar la tasca de les autoritats

[90]Conceptos jurídicos (2024). *Delitos contra la libertad sexual*. Conceptosjurídicos.com https://www.conceptosjuridicos.com/delitos-contra-la-libertad-sexual/

[91] Fierro, D. (2024). *La (in)existente necesidad de regular delitos cometidos con inteligencia artificial.* Economist & Jurist.

jurídiques per la seva qualificació i penalització, a més de constituir una nova forma de manipulació dels sistemes de justícia.

El principal risc al qual s'enfronta la Justícia és la falsificació de proves entorn del *deepfake* pel fet que –com s'ha esmentat al llarg del treball– aquests poden ser presentats com proves legítimes i viciar declaracions dels testimonis per haver visualitzat o escoltat gravacions manipulades per IA, les quals creuen que són reals. Això deriva en una major inversió de temps, diners i esforç dels operadors jurídics per verificar i autentificar les proves abans de ser admeses pels tribunals.[92] Sumat a totes aquestes adversitats, es troben les novetats que els *deepfakes* han introduït en la comissió de ciberviolència masclista *(remissió al punt 3.4)*.

Enfront d'aquesta situació en auge, s'han posat en marxa algunes accions per part de les autoritats judicials i fiscals, tot i que encara és necessari invertir esforços en aquesta matèria, pel fet que ha capgirat la realitat jurídica existent.

En primer lloc, en les bases i temari de la convocatòria 2023-2024 de les oposicions per jutges i fiscals,[93] en el tema 30 de Dret penal, s'inclouen els delictes contra la dona com l'assetjament o la divulgació no consentida d'imatges o gravacions íntimes (*sexting* secundari); a més, en la pregunta 69 del primer exercici celebrat el 18 de febrer del 2024 per aquestes mateixes oposicions, es mencionen tant el *sexting* com el *grooming*. A més el Pla Docent de Formació Inicial de la 74a Promoció de la Carrera Judicial introdueix la formació en IA en diversos apartats: d'una banda, en l'àrea de Dret Constitucional i de la Unió Europea com a activitat complementària s'inclou el tema "Intel·ligència Artificial i Drets Fonamentals" on s'exposa la IA com eina de doble tall –com una amenaça, però també com oportunitat de garantia dels drets fonamentals dels ciutadans–; d'altra, en el Bloc III com a matèria troncal s'imparteix el tema "Revolució digital en l'àmbit jurídic: Blockchain i Intel·ligència Artificial".[94] Finalment, pel que fa als jutjats especialitzats (art. 98 LOPJ), no s'ha localitzat cap òrgan judicial que tingui atribuït en exclusiva el coneixement de matèries

[92] Bello, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI*, 219-248. Colex.
[93] Acuerdo de 27 de octubre de 2023, de la Comisión de Selección a la que se refiere el artículo 305 de la Ley Orgánica del Poder Judicial, por el que se convocan pruebas selectivas para la provisión de plazas de alumnos y alumnas de la Escuela Judicial, para su posterior acceso a la Carrera Judicial por la categoría de Juez/a, y plazas de alumnos y alumnas del Centro de Estudios Jurídicos, para su posterior ingreso en la Carrera Fiscal por la categoría de Abogado/a Fiscal, BOE, núm 262, de 2 de noviembre de 2023.
[94] Escuela Judicial (2024). *Plan docente de formación inicial 74ª Promoción Carrera Judicial: curso 2024-2025*. Poder judicial.

relacionades amb la ciberdelinqüència ni amb la IA –ja que aquests majoritàriament versen sobre família i violència contra la dona–.[95]

Tenint en compte aquesta realitat, es creu oportú que hi hagi una mínima formació en IA en el temari de les oposicions, incidint en com la IA pot propiciar la comissió de delictes en l'àmbit penal –no només des de la perspectiva constitucional i dels drets fonamentals com s'havia anat fent– i, sobretot, incidir en els *deepfakes* com a una nova tipologia delictiva que –com s'ha esmentat a l'anterior punt– hauria de regular-se en els delictes contra la integritat moral. Es proposa la implementació de la IA en els jutjats per verificar el material audiovisual i probatori –és a dir, detectar la IA amb la mateixa IA– sobretot en els casos de possibles *deepfakes* aportats com a proves aparentment legítimes. Qüestió més complexa de contrarestar són els *deepfakes* emprats per viciar les declaracions dels testimonis –tot i que les declaracions viciades són molt anteriors a l'existència de la IA–; en aquests casos, es valora la possibilitat de fer campanyes de sensibilització de testimonis sobre la possibilitat que se'ls puguin haver mostrat abans de la seva declaració imatges, vídeos, textos o àudios manipulats mitjançant IA, per la qual cosa han de consultar-ho amb el seu lletrat per dur a terme les actuacions pertinents sobre aquests suports. És necessària una especialització dels jutges espanyols en la matèria i, per això, es valora la possibilitat de crear jutjats especialitzats (art. 98 LOPJ) en Criminalitat Informàtica –tal com ha vingut realitzant des de fa aproximadament tretze anys la Fiscalia–. Endemés, es considera que els jutges penals que es trobin front un cas en què hi hagi indicis d'ús d'IA –per exemple en un cas amb presumptes *deepfakes*– haurien de designar un pèrit d'ofici amb els coneixements científics suficients en IA i *deepfakes*, seguint l'art. 456 LECrim: *"El jutge acordarà l'informe pericial quan, per conèixer o apreciar algun fet o circumstància important al sumari, fossin necessaris o convenients coneixements científics o artístics."*

Fent referència expressa a la formació impartida a la Fiscalia General de l'Estat, cal destacar –a més de diversos cursos en IA– la formació continuada 2022 de la carrera fiscal en la qual es va desenvolupar l'activitat "IA i justícia". Un dels grans avenços de la Fiscalia en aquest tema és la creació de la Fiscalia de Criminalitat Informàtica mitjançant la Instrucció 2/2011, d'11 d'octubre, sobre el Fiscal de Sala de Criminalitat Informàtica i les seccions de criminalitat informàtica de les Fiscalies. En el seu marc competencial s'inclouen una sèrie de delictes els quals s'han relacionat amb els tipus de ciberviolència masclista *(remissió al punt*

[95] Poder Judicial (s.d.) *Juzgados especializados.* https://www.poderjudicial.es/cgpj/es/Servicios/Demarcacion-y-Planta-Judicial/Juzgados-especializados

2.4): el delicte de descobriment i revelació de secrets de l'art. 197 CP –podent-se incloure en aquest el *sexting* secundari, la sextorsió i el *doxing*–; el delicte de *child grooming* tipificat en l'art. 183 CP; delictes d'amenaces i coaccions penats als arts. 169 i ss. CP comesos a través de les TIC sempre que això fos determinant en l'activitat delictiva i generés especial complexitat en la investigació criminal –en aquesta categoria es podria incloure la sextorsió i el cibercontrol cap a les noies–; delictes d'apologia o incitació a la discriminació, l'odi i violència penats en l'art. 510 CP comesos a través de les TIC sempre que això fos determinant en l'activitat delictiva i generés complexitat en la investigació criminal –es considera que hi té cabuda la cibermisogínia–; també tenen competència respecte dels delictes contra la integritat moral de l'art. 173.1 CP comesos a través de les TIC sempre que això fos determinant en l'activitat delictiva i generés especial complexitat en la investigació criminal –aquí serien competents per tractar el *body-shaming, slut-shaming,* la cibermisogínia, la sextorsió i el *doxing*–; finalment, es dona una clàusula de tancament en què s'inclou qualsevol tipus delictiu en l'execució del qual hagi estat determinant l'ús de les TIC i això generi especial complexitat en la investigació criminal. És important remarcar el fet que en aquesta Instrucció no es considera la IA –ja que és anterior a l'aparició d'aquesta– i, per tant, no s'inclouen els *deepfakes;* no obstant això, es considera que els *deepfakes* es trobarien dins de les competències de la Fiscalia de Criminalitat Informàtica pel fet que –tal com s'esmenta en el punt anterior– s'hauria de tipificar amb els delictes contra la integritat moral de l'art. 173 CP, els quals s'ha observat que són competència d'aquesta Fiscalia. També es podria declarar competent en el cas dels *deepnudes* de menors, ja que dins de les seves competències inclou el delicte de pornografia infantil quan pel seu desenvolupament i/o execució de l'activitat delictiva s'utilitzin les TIC.

Partint del recentment exposat, es recomana que enfront dels possibles casos de *deepfakes* es doni una col·laboració entre la Fiscalia de Criminalitat Informàtica i la Fiscalia de Violència sobre la Dona, per aportar especialització en IA però amb perspectiva de gènere. En relació amb aquest fet, es considera oportuna l'especialització d'alguns dels fiscals de la Fiscalia de Criminalitat Informàtica en IA –i, en concret, en *deepfakes*–. Finalment i com s'apuntava amb antelació, es proposa fer menció expressa als *deepfakes* en el llistat de delictes sobre els quals té competència la Fiscalia de Criminalitat Informàtica –enumerats en la Instrucció 2/2011, anteriorment citada–, concretament com a tipus específic dels delictes contra la integritat moral de l'art. 173.1 CP expressats en tal Instrucció.

5- CONCLUSIONS

1- En primera instància, entorn les controvèrsies sobre la terminologia, s'ha optat per parlar de violència masclista per considerar-se un concepte que engloba un nombre més extens conductes i, per tant, més adient en concordança amb les conductes tractades en el treball –en el mateix sentit, s'opta pel terme ciberviolència masclista quan aquesta s'exerceix a través de les TIC–.

2- Quant a la regulació de la ciberviolència masclista, destaca la manca d'un títol específic pels ciberdelictes; a més, moltes d'aquestes conductes són extrapenals –a excepció del *sexting* secundari i *revenge porn* (art. 197.7 CP) i *online grooming* (art. 183 CP)–. A través de la taula d'elaboració pròpia del punt 2.4, s'ha observat com moltes d'aquestes conductes extrapenals no tenen un encaix adequat en el CP tal com està redactat actualment, pel fet que aquestes encaixen en diversos delictes, però alhora no acaben d'inserir-se a cap: o bé perquè els tipus del CP no encaixen amb la fenomenologia delictiva d'aquestes conductes –ja que alguns tipus necessitarien modificacions– o bé perquè els requisits perquè es donin tals conductes estan disseminats en diversos articles del CP. Tot i la manca de regulació específica d'aquestes conductes en el CP, s'adverteix com la llei s'adapta als canvis socials incloent-se referències a les violències sexuals en l'àmbit digital –amb especial referència a la sextorsió– en la Llei Orgànica 10/2022, de 6 de setembre, de garantia integral de la llibertat sexual. Destaca com les estadístiques denoten un increment d'aquesta violència on ser jove i ser dona són factors clau, tot i que l'escassetat d'estadístiques específiques dificulta tenir una imatge clara del fenomen; llavors, es considera necessari arribar a un consens sobre si aquestes conductes mereixen una tipificació específica o en quin dels tipus penals proposats es podrien inserir.

3- Amb la irrupció de la IA –en la seva modalitat d'IA generativa– s'intensifica la ciberviolència masclista cap a les dones, donant lloc als *deepfakes* –també en la seva modalitat de *deepnudes*–. Els *deepfakes* han transformat la ciberviolència masclista, essent una nova eina per exercir aquest tipus de violència per les seves finalitats malicioses –molt més intenses en el cas dels *deepnudes* pel seu hiperrealisme–. Destaca la deficient regulació dels *deepfakes*: d'una banda, el Reglament d'IA només els defineix i estableix obligacions de transparència –sense establir responsabilitats, a diferència de la IA d'alt risc–; d'altra, l'únic intent de regulació dels *deepfakes* a Espanya sorgeix de la Proposició de Llei Orgànica del Grup Sumar. Al llarg de l'explicació s'ha argumentat que tot i la necessitat de crear un tipus

específic en el CP per castigar els *deepfakes* i de regulació en àrees complementàries –com es fa amb la Proposició de Llei Orgànica–, no es pot seguir la línia d'aquesta Proposició de Llei Orgànica quant a la tipificació dels *deepfakes* com a delicte d'injúries. Consegüentment, s'opta per tipificar-ho com a delicte contra la integritat moral –proposant-se una possible redacció d'un nou tipus penal en un nou art. 173.1 II CP– per ser més proporcional amb la gravetat de la conducta, no havent-se de fer una conciliació prèvia amb el querellat, ser un tipus més ampli i estar en concordança tant amb la resta de conductes de ciberviolència masclista com amb les imputacions previstes en els casos mediàtics de *deepfakes* a Espanya. Tampoc és adient tipificar-ho com a delicte de suplantació d'identitat per ser anacrònic i no inserir-se la conducta dins el tipus penal. Pel que fa als problemes d'autoria relacionats amb els *deepfakes,* es considera possible l'atribució de responsabilitat penal tant dels titulars dels comptes de les xarxes socials on es creïn o difonguin aquests continguts com dels propietaris de les plataformes d'IA i de les plataformes en què es difonguin aquests. Cal també remarcar la possibilitat de concurs real de delictes amb els delictes de lesions psíquiques, contra la llibertat sexual i contra l'honor.

4- Respecte de la preparació dels jutges, no es desprèn que hi hagi formació en com el Dret penal es relaciona amb la IA, amb la consegüent aparició dels *deepfakes;* a més, manca l'existència d'òrgans especialitzats en aquestes qüestions. En el cas de la Fiscalia, s'imparteixen cursos i formacions i es determina que dins les competències de la Fiscalia de Criminalitat Informàtica es podrien inserir els *deepfakes*, pel fet que aquests són competents per conèixer dels delictes contra la integritat moral comesos a través de les TIC sempre que això fos determinant en l'activitat delictiva i generés especial complexitat en la investigació criminal; així i tot, es creu adient la col·laboració amb la Fiscalia de Violència sobre la Dona, per assolir una especialització en IA però amb perspectiva de gènere.

El present treball ha permès posar de manifest l'evolució de la ciberviolència masclista fins a la seva situació actual, a causa de la disrupció de la IA. En concret s'han exposat els riscos i problemes que planteja aquesta nova tecnologia i la incertesa entorn la regulació dels *deepfakes.* Gràcies a aquest treball, s'ha aprofundit en els debats doctrinals existents i s'espera haver pogut obrir noves línies d'investigació futures per abordar el tema.

7- REFERÈNCIES BIBLIOGRÀFIQUES

– Aider, H., Patrini, G., Cavalli, F., Cullen, L., (Deeptrace Labs). (2019). *The State of Deepfakes: Landscape, Threats, and Impact.*

– Ansón, R. (2023) *Deepfake y Legislación: retos y proposición de Ley Orgánica.* Bufete Mas y Calvet.

– Apolo, C. (2023) Lo que se sabe hasta el momento del caso de los falsos desnudos de las menores en Almendralejo (Badajoz). *elEeconomista.es.*

– Bañuelos, J. (2020). "Deepfake: la imagen en tiempos de la posverdad." *Revista Panamericana de Comunicación,* 2(1), 51-61.

– Bello, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI*, 219-248. Colex.

– Bigas, N. (2023) *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos.* UOC.

– Coloma, M. A. (2024). Caso de las fotos trucadas con IA en Utebo: las víctimas de los falsos desnudos son 5 chicas. *Heraldo.*

– Comisión Europea (2024). *Ley de IA.*
https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai

– Comisión Europea (2018) Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan coordinado sobre la inteligencia artificial.

– Conceptos jurídicos (2024). *Delitos contra la libertad sexual.* Conceptosjurídicos.com
https://www.conceptosjuridicos.com/delitos-contra-la-libertad-sexual/

– Conceptos jurídicos (2024). *La injuria.* Conceptosjurídicos.com
https://www.conceptosjuridicos.com/injuria/

– Consejo de Europa (2018). Mapping study on cyberviolence. Cybercrime Convention Committee (TCY). Working Group on cyberbullying and other forms of violence, especially against women and children.

– Delegación del Gobierno contra la Violencia de Género. (s.d.) *Violencia de género digital.*
https://violenciagenero.igualdad.gob.es/informacionUtil/comoDetectarla/VG_Digital/home.htm.

– Departament d'Interior de la Generalitat de Catalunya (s.d.), *Violència masclista.*
https://interior.gencat.cat/es/arees_dactuacio/seguretat/violencia_masclista/

– Duque, I. (2020) *Guía didáctica conectar sin que nos raye.* Ayuntamiento de Andújar, Centro Municipal de información a la mujer (CMIM).
– EFE. (2024). Las víctimas de los falsos desnudos de Almendralejo estudian propuesta de acuerdo de la Fiscalía. *EFE*.
– Escuela Judicial (2024). *Plan docente de formación inicial 74ª Promoción Carrera Judicial: curso 2024-2025*. Poder judicial.
– Estebánez, I. (2018) *La ciberviolencia hacia las adolescentes en las redes sociales: guía didáctica.* Instituto Andaluz de la Mujer.
– EU Artificial Intelligence Act (2024). *Resumen de alto nivel de la Ley AI.* https://artificialintelligenceact.eu/es/high-level-summary/
– European Parliamentary Research Service (2021). *Combating gender-based violence: Cyber violence European added value assessment.* European Parliament.
– European Parliamentary Research Service (EPRS) (2021) *Tackling deepfakes in European policy.* European Parliament. DOI: 10.2861/325063
– Felip, D. i Ragués, R. (2018). "Torturas y otros delitos contra la integridad moral". *Lecciones de Derecho Penal Parte Especial* (Sexta Edición), 117-131. Atelier.
– Fierro, D. (2023) "La necesidad de sancionar penalmente la difusión de ciertas imágenes creadas con inteligencia artificial". *Diario LA LEY,* Nº 77, Sección Ciberderecho, 3 de Noviembre de 2023, LA LEY.
– Fierro, D. (2024). *La (in)existente necesidad de regular delitos cometidos con inteligencia artificial.* Economist & Jurist.
– Fiscalía General del Estado (2022). *Memoria Anual de la Fiscalía General del Estado 2021*. Ministerio de Justicia.
– Gavilán, M. (2018). "Violencia de género digital: el delito de ciberacoso. Breve resumen de jurisprudencia. Asistencia a la víctima". *Servicios sociales y política social,* (116), 53-61.
– González, I. (2023) "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes". *IUS ET SCIENTIA*, 9 (2), 157-180.
– González, L. (2023) *Comprendiendo la asombrosa IA: Una guía definitiva para entender la inteligencia artificial.* Aprende IA.
– Home Security Heroes (s.d.) *State of Deepfakes 2023. Realities, Threats, and Impact.* Home Security Heroes.
– Instituto Europeo de Igualdad de Género (2017). *La ciberviolencia contra mujeres y niñas.* Oficina de Publicaciones de la Unión Europea, 1-11.

– Instituto Nacional de Estadística (2023). Notas de prensa. Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares Año 2023.
– Linares, E.; Royo, R.; Silvestre, M. (2019). "El ciberacoso sexual y/o sexista contra las adolescentes. Nuevas versiones online de la opresión patriarcal de las sexualidades y corporalidades femeninas". *Doxa Comunicación,* 28, 201-222.
– Llorens, M. (2022) "Avances legislativos y retos en materia de Violencia de Género Digital". *Nuevas tecnologías 2022*, 231-248. Tirant lo Blanch.
– Lloria, P. (2014). "Violencia de género en el entorno digital". *Crímenes y castigos: miradas al Derecho penal a través del arte y la cultura*, 547-562. Tirant lo Blanch.
– López, S. (2023). "Inteligencia artificial ¿una herramienta de doble filo? Especial referencia a su aplicación en el ámbito de la violencia de género". *Aspectos jurídicos de actualidad en el ámbito del Derecho digital*, 141-164. Tirant lo Blanch.
– Martín, R. (2021). "Violencia de género en la era digital: el delito de sexting". *Feminismo digital: violencia contra las mujeres y brecha sexista en Internet*, 421-439.
– Martínez, M. I. (2015) "Las nuevas tecnologías como herramientas de prevención y actuación frente a la violencia de género". *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención*, 111-226. Universidad Internacional de Andalucía.
– Moral, G. (2024). Un acuerdo podría evitar el juicio por el caso de los falsos desnudos por IA en Almendralejo. *el Periódico Extremadura.*
– Muniesa, P.; Herrera, T.D.; Guerrero, J.; Martínez, F.; Rubio, M.; Gil, V.; Santiago, A.M. i Gómez, M.A. (2023). *Informe sobre la cibercriminalidad en España.* Ministerio del Interior.
– Observatorio Nacional de Tecnología y Sociedad (2022). *Violencia de género: una realidad invisible 2022*. Ministerio de Asuntos Económicos y Transformación Digital.
– Oyarzábal, N. i Pérez, R. (2023) *Deepfake vs. Derecho al honor, intimidad y propia imagen.* Cuatrecasas.
–Poder Judicial (s.d.) *Juzgados especializados.* https://www.poderjudicial.es/cgpj/es/Servicios/Demarcacion-y-Planta-Judicial/Juzgados-especializados
– Público. (2023). La app de falsos desnudos no tiene responsabilidad penal, pero podría ser acusada de negligencia. *Público*.
– Público. (2024). Condenan a un joven de 18 años por difundir imágenes falsas de compañeras desnudas generadas por IA. *Público*.

– Rodríguez, J. & Rodríguez, L. (2022). "Violencia de género en soportes digitales". *Opción: Revista de Ciencias Humanas y Sociales,* (29), 396-416.
– Sala, R. (2019). "La violencia de género digital: tratamiento jurídico y percepción social". *La Ley Derecho de Familia: Revista jurídica sobre familia y menores,* (23), 34-40.
– Secretaría General del Congreso de los Diputados (2021), Registro General, Entrada 79830.
– Simó, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho". *InDret,* 493-515.
– Sorrentino, C. (2024) *Intelligenza artificiale: cosa prevede la normativa italiana.* Osservatori.net.
– Torres, C., Robles, J.M. i de Marco, S. (2014). *El ciberacoso como forma de ejercer la violencia de género en la juventud: Un riesgo en la sociedad de la información y el conocimiento.* Ministerio de Sanidad, Servicios Sociales e Igualdad.
– Valdés, B. (2024) Fiscal Elvira Tejada, sobre el uso de IA para simular la identidad: «No tiene una respuesta adecuada en el Código Penal». *Confilegal*.
– Van der Wilk, A. (2021). *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología.* Consejo de Europa.
– Vera, K. (2021). *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos.* OAS Documentos oficiales.

8- ANNEX DE LEGISLACIÓ

– Acuerdo de 27 de octubre de 2023, de la Comisión de Selección a la que se refiere el artículo 305 de la Ley Orgánica del Poder Judicial, por el que se convocan pruebas selectivas para la provisión de plazas de alumnos y alumnas de la Escuela Judicial, para su posterior acceso a la Carrera Judicial por la categoría de Juez/a, y plazas de alumnos y alumnas del Centro de Estudios Jurídicos, para su posterior ingreso en la Carrera Fiscal por la categoría de Abogado/a Fiscal, BOE, núm 262, de 2 de noviembre de 2023.
– Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.
– Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE, núm. 281, de 24 de noviembre de 1995.

– Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, BOE, núm 313, de 29 de diciembre de 2004.
– Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, BOE, núm. 215, de 7 de septiembre de 2022.
– Ley 7/2018, de 30 de julio, por la que se modifica la Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género, BOE, núm. 207, de 27 de agosto de 2018, páginas 84908 a 84930.
– Organización de Naciones Unidas (1994). Declaración sobre la eliminación de la violencia contra la mujer. Resolución de la Asamblea General 48/104 del 20 de diciembre de 1993.
– Parlamento Europeo. Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)), 14 de junio de 2023.
– Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, Boletín Oficial de las Cortes Generales, Núm 23-1, de 13 de octubre de 2023.
– Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal, BOE, núm. 260, de 17 de septiembre de 1882.
– Reglamento de Inteligencia Artificial. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))