
This is the **published version** of the bachelor thesis:

Maeso Chantrero, Gerard; Robert Guillén, Santiago, dir. La intel·ligència artificial generativa i les vulneracions del dret de la personalitat : anàlisi jurídica dels deepfakes i el seu impacte en la protecció de la imatge i la veu de figures públiques en l'àmbit esportiu europeu. 2025. (Grau en Dret i Grau en Relacions Laborals)

This version is available at <https://ddd.uab.cat/record/319320>

under the terms of the  license



**La intel·ligència artificial generativa i les vulneracions del dret de la
personalitat: anàlisi jurídica dels *deepfakes* i el seu impacte en la
protecció de la imatge i la veu de figures públiques en l'àmbit esportiu
europeu**

Treball de Final de Grau

Facultat de Dret UAB

AUTOR/A: GERARD MAESO CHANTRERO

TUTOR/A: SANTIAGO ROBERT GUILLÉN

GRAU: DOBLE GRAU EN DRET I RELACIONS LABORALS

DATA: 13 DE MAIG DE 2025

RESUM

Són ja diversos i cada cop més habituals els casos en els quals s'imita la veu i/o imatge de figures públiques del món esportiu mitjançant intel·ligències artificials generatives per fer-ne tota mena d'ús. Aquest material multimèdia generat via IA es coneix com “*deepfakes*” quan és utilitzat com el propi nom indica en la seva traducció, com a “engany profund” amb fins contraris a aquells lícits. Aquestes possibilitats creixents que ofereixen les IA generatives i que són a l'abast de tothom sent moltes d'elles gratuïtes poden posar en risc i vulnerar els drets de la personalitat de les persones, utilitzant per posar un exemple, l'imatge i veu d'algu conegut per promocionar un producte o servei sense el consentiment ni la pertinent retribució de la persona en qüestió.

Tenint en compte les característiques de la IA i el creixement tecnològic que presenta el paradigma actual, aquestes deixen desactualitzades amb facilitat moltes de les normes legals que van elaborant-se. És per aquest motiu que s'inicia aquest treball centrant-nos dins del marc acotat esportiu i comercial europeu buscant entendre el funcionament dels principis legals de caràcter més atemporal vinculats amb el progrés de les IA que en permetin una regulació que no quedi desfasada (consentiment, responsabilitat i aquells vinculats amb drets fonamentals de la personalitat). A través d'aquest estudi s'analitzarà el marc jurídic europeu existent i la seva aplicabilitat als “*deepfakes*” identificant vulneracions específiques dels drets d'imatge i veu de casos reals.

Un cop analitzada la norma, es busca plantejar possibles solucions a través de marcs legals més adaptables i, des d'una vessant comercial, idear sistemes de retribució més justos i eficients per a l'explotació dels drets d'imatge i veu i, que a la vegada, respectin aquests drets de la personalitat de les figures públiques del món de l'esport que vegin imitada la seva veu i/o imatge a través de les IA generatives. Per fer-ho s'explorà la possibilitat d'idear a través de la utilització de tecnologia *blockchain* i *smartcontracts*, un sistema per a l'elaboració de contractes de cessió i ús d'aquests drets.

Paraules clau: *deepfake*, IA, drets de la personalitat, dret d'imatge i veu, AI Act, GDPR, esport, *blockchain*.

ABSTRACT

There are already several and increasingly common cases in which the voice and/or image of public figures from the world of sport are imitated by artificial generative intelligences to make all kinds of use. This AI-generated multimedia material is known as ‘deepfakes’ when it is used, as the name itself indicates in translation, as ‘deep deception’ for purposes contrary to those that are lawful. These growing possibilities offered by generative *IAs and which are available to everyone, many of them free of charge, can put at risk and violate the personality rights of individuals, using, for example, the image and voice of someone known to them to promote a product or service without the consent or the relevant remuneration of the person in question.

Taking into account the characteristics of AI and the technological growth of the current paradigm, many of the legal regulations that are being developed are easily outdated. It is for this reason that this work begins by focusing on the European sporting and commercial framework, seeking to understand the functioning of the most timeless legal principles linked to the progress of AIs that allow for regulation that is not outdated (consent, liability and those linked to fundamental rights of the personality). This study will analyse the existing European legal framework and its applicability to deepfakes, identifying specific violations of image and voice rights in real cases.

Once the regulations have been analysed, the aim is to propose possible solutions through more adaptable legal frameworks and, from a commercial perspective, to devise fairer and more efficient remuneration systems for the exploitation of image and voice rights, while at the same time respecting the personality rights of public figures from the world of sport who see their voice and/or image imitated through generative AI. To do so, we will explore the possibility of devising, through the use of blockchain technology and smart contracts, a system for drawing up contracts for the assignment and use of these rights.

Keywords: deepfake, AI, personality rights, image and voice rights, AI Act, GDPR, sport, blockchain.

Agraïments: al tutor d'aquest treball, el Doctor Santiago Robert Guillén per la magnífica guia a l'hora de dur a terme aquest estudi, a tots els professors que han format el meu criteri jurídic al llarg de la carrera, a la família i amics que m'han recolzat i despertat el meu interès per aquest camp del dret i, finalmet, al meu gos Jax i la meva gata Nala per les hores de companyia durant l'elaboració d'aquest treball.

ABREVIATURES

AEPD	Agència Espanyola de Protecció de Dades
AFA	<i>Asociación del Fútbol Argentino</i>
AI Act	Reglament 2024/1689
Art.	Article
AESIA	Agència Espanyola de Supervisió d'Intel·ligència Artificial
BOE	Boletín Oficial del Estado
CE	Constitució espanyola
CEDH	Conveni Europeu de Drets Humans
CNN	Xarxes neuronals convolucionals
COI	Comitè Olímpic Internacional
CNIL	<i>Commission Nationale de l'Informatique et des Libertés</i>
F1	Fórmula 1
FA	<i>Football Association</i>
FIFA	<i>Fédération Internationale de Football Association</i>
FTO	<i>Fan Token Offering</i>
GAN	Xarxes neuronals generatives adversatives

GDPR	Reglament General de Protecció de Dades
IA	Intel·ligència Artificial
LIA	<i>Legitimate Interest Assessment</i>
OMPI	Organització Mundial de la Propietat Intel·lectual
ONU	Organització de les Nacions Unides
RNN	Xarxes neuronals recurrents
STS	Sentència
TEDH	Tribunal Europeu de Drets Humans
TJUE	Tribunal de Justícia de la Unió Europea
UE	Unió Europea
UEFA	Union of European Football Associations
UNESCO	<i>United Nations Educational, Scientific and Cultural Organization</i>
AEPD	Agència Espanyola de Protecció de Dades
AFA	<i>Asociación del Fútbol Argentino</i>
AI Act	Reglament 2024/1689
Art.	Article
AESIA	Agència Espanyola de Supervisió d'Intel·ligència Artificial

TAULA DE CONTINGUTS

1. **Introducció**
2. **Impacte de la intel·ligència artificial en els drets d'imatge i veu en l'àmbit esportiu europeu: anàlisi jurídica i ètica**
 - 2.1. Efectes de la IA generativa en la identitat dels esportistes: qüestions ètiques emergents
 - 2.2. Usos i límits de la IA en els drets de la personalitat: delimitació entre *deepfakes* i contingut identificat
 - 2.3. Règim legal europeu aplicable a l'ús d'IA en l'esport
 - 2.4. Casos d'usos i vulneracions de drets de la personalitat d'esportistes a través de *deepfakes*
3. **Nous horitzons i reptes per als esportistes en l'era digital més enllà de les vulneracions per *deepfakes***
 - 3.1. Exposició pública amplificada i pressió social sobre els drets d'imatge i veu dels esportistes
 - 3.2. Limitacions tecnològiques i desafiaments de prevenció enfront de la manipulació de dades biomètriques
 - 3.3. Impacte i conseqüències econòmiques indirectes dels *deepfakes* en el valor de mercat dels esportistes
4. **Estudi jurídic de les vulneracions de drets d'imatge i veu de casos comentats**
 - 4.1. Cas Eddie Irvine v. Talksport Ltd
 - 4.2. Cas Lionel Messi i *deepfake Wildcat Dive*
 - 4.3. Cas Southgate
 - 4.4. Cas Mario Draghi

5. Propostes de futur per a la protecció dels drets d'imatge i veu dels esportistes

5.1. Propostes de regulacions futures i guies de bones pràctiques en l'àmbit esportiu

5.2. Viabilitat jurídica del blockchain en la protecció dels drets de la personalitat i la protecció econòmica dels drets d'imatge i veu en l'era digital de la IA

6. Conclusions

7. Bibliografia

1. Introducció

La ràpida evolució de la intel·ligència artificial (IA) ha transformat nombrosos àmbits, incloent-hi la creació d'imatges i contingut multimèdia, amb un impacte notable en el món de l'esport. La combinació de tècniques tradicionals, com la captació d'imatges en retransmissions o la fotografia digital, amb la IA ha generat noves possibilitats, especialment amb tecnologies com els *deepfakes*. Aquestes eines permeten crear representacions hiperrealistes d'esportistes d'elit, replicant trets físics, veu i moviments, cosa que qüestiona la veracitat del contingut digital i planteja dilemes legals i ètics sobre la titularitat i protecció dels drets d'imatge.

Aquest tema ha estat escollit perquè és el punt de trobada entre el caràcter innovador i la rellevància acadèmica de la matèria amb el meu interès personal pel camp del dret esportiu, especialització dins del món del dret que més m'interessa i a la que em vull dedicar professionalment. Dins del dret, desperta el meu interès el dret d'imatge i com es regula i protegeix aquest, sent idoni per tant acotar aquest treball a l'àmbit esportiu europeu que es tracta d'un context sobre el qual tinc coneixements i una especial vocació.

La creixent utilització no autoritzada de la imatge i veu de figures públiques, sovint en campanyes comercials, evidencia la manca d'un marc legal sòlid que protegeixi els drets de la personalitat dels esportistes. Aquest camp emergent, poc regulat, ofereix un terreny fèrtil per a l'anàlisi jurídica, especialment en l'àmbit europeu, on la intersecció entre tecnologia i dret és un repte actual.

La metodologia del treball combina l'anàlisi de casos rellevants amb un enfocament comparatiu, passant pel filtre normatiu europeu i integrant doctrina i jurisprudència. S'examinen situacions concretes de vulneracions de drets d'imatge i veu mitjançant *deepfakes*, avaluant-ne les conseqüències en els drets de la personalitat i en el mercat esportiu i comercial europeu.

L'objectiu principal és aprofundir en el coneixement jurídic d'aquestes tecnologies generatives, analitzant les vulneracions que poden generar, el seu impacte tant en els drets d'imatge i veu dels esportistes com en el seu valor comercial i rendiment esportiu. Havent analitzat aquestes vulneracions es procedirà a valorar les respostes legals i doctrinals

existents. Aquest cas té valor perquè aborda un problema real i urgent, amb implicacions tant individuals com col·lectives que afecten tot l'ecosistema del món esportiu a Europa.

El treball s'estructura en diversos capítols: el primer, aquesta mateixa introducció; el segon contextualitza la IA en l'esport des d'un punt de vista legal i ètic mostrant com la tecnologia *deepfake* ha creat situacions de vulneracions; el tercer analitza des d'una òptica més tècnica les vulneracions generades per *deepfakes* i quin impacte econòmic i legal sobre el tractament de dades poden generar; el quart estudia casos concrets anunciats al segon capítol entrant en valoracions jurídiques i quin tractament jurisprudencial s'ha aplicat o seria aplicable dins el marc normatiu europeu; i el cinquè proposa solucions futures, com l'ús de *blockchain* per gestionar drets d'imatge.

Degut a la limitació del format d'aquest treball, es finalitza amb el plantejament de futures línies de recerca, com l'aplicació de tecnologies emergents per garantir una compensació justa i automatitzada, obrint la porta a futures investigacions sobre models més transparents de protecció i explotació comercial dels drets d'imatge d'esportistes en l'era digital.

2. Impacte de la intel·ligència artificial en els drets d'imatge i veu en l'àmbit esportiu europeu: anàlisi jurídica i ètica

2.1 - Efectes de la IA generativa en la identitat dels esportistes: qüestions ètiques emergents

La irrupció de la intel·ligència artificial generativa en l'àmbit esportiu ha revolucionat la gestió i percepció dels drets de la personalitat, sent objecte d'estudi en aquest treball en particular el dret d'imatge i veu dels esportistes, qui, com a figures públiques, són persones en una posició d'especial vulnerabilitat davant aquestes tecnologies pel simple fet de l'interès que el seu estatus genera. Els avanços en tecnologia d'algorismes com les xarxes neuronals adversatives (Generative Adversarial Networks, GANs)¹ permeten la creació de representacions hiperrealistes que repliquen amb precisió la fisonomia, els rostres, gestos i locucions de persones; permeten replicar dades biomètriques amb cada cop més i més precisió plantejant desafiaments ètics i jurídics d'enorme magnitud.

¹ ALONSO, C. (18/11/2024). *Deepfake: ¿qué es y cómo detectarlo?*. UNIR Revista. <https://www.unir.net/revista/derecho/deepfake-que-es/>

Els sistemes d'IA plantegen nous tipus de qüestions ètiques que inclouen, però no es limiten a, el seu impacte en la presa de decisions, l'ocupació i el treball, la interacció social, l'assistència sanitària, l'educació, els mitjans de comunicació, l'accés a la informació, la bretxa digital, les dades personals i la protecció del consumidor, el medi ambient, la democràcia, l'Estat de Dret, la seguretat i la policia, l'ús dual i els drets humans i les llibertats fonamentals inclosa la llibertat d'expressió, la privacitat i la no discriminació. A més, els nous reptes ètics es creen a partir del potencial dels algoritmes d'IA per reproduir i reforçar els biaixos existents, i per tant per exacerbar les formes de discriminació ja existents, els prejudicis i estereotips. Algunes d'aquestes qüestions estan relacionades amb la capacitat dels sistemes d'IA per dur a terme tasques que abans només els éssers vius podien fer, i que en alguns casos fins i tot es limitaven a éssers humans.

Aquestes característiques confereixen als sistemes d'IA un paper profund i nou en les pràctiques humanes i la societat, així com en la seva relació amb el medi ambient i els ecosistemes, creant un nou context perquè els nens i joves creixin, desenvolupin una comprensió del món i d'ells mateixos, entenguin críticament els mitjans i la informació i aprenguin a prendre decisions. A llarg termini, els sistemes d'IA podrien desafiar el sentit especial de l'experiència i l'agència dels humans, plantejant preocupacions addicionals sobre, entre altres coses, l'autocomprensió humana, la interacció social, cultural i ambiental, l'autonomia, l'agència, el valor i la dignitat.²

Aquesta pèrdua de control sobre la pròpia identitat constitueix una erosió de l'agència individual, un fenomen especialment crític en l'esport, on la reputació és un actiu intangible essencial, l'autenticitat de l'atleta és un pilar de la seva credibilitat. Això pot tenir una implicació molt profunda i subjectiva en el públic que el percep d'una forma alterada i esbiaixada degut a vulneracions que aquest ha patit via *deepfakes*, portant entre altres coses, a possibles afectacions psicològiques que afectin el seu rendiment, cancel·lacions de campanyes publicitàries per una mala reputació generada artificialment, afectació a la reputació i imatge del club al que pugui representar l'esportista fent-ne una qüestió que implica a més actors, que l'esportista no sigui considerat per un possible contracte, mala reputació i campanyes de desprestigi buscant afectar el seu rendiment esportiu... i un llarg etcètera de factors rellevants tant a nivell ètic com jurídic que posen de manifest la perillositat d'un ús descontrolat d'aquesta tecnologia.

²UNESCO. (25/06/2021) *Recomanació sobre l'ètica de la intel·ligència artificial*. 2021 pp. 5 i 6
<https://unesdoc.unesco.org/ark:/48223/pf0000377897>

Un exemple paradigmàtic de l'anterior seria la creació d'un vídeo fals en el qual un futbolista d'elit, com Lionel Messi, aparegués confessant haver fet ús de substàncies prohibides. Encara que el contingut fos posteriorment desmentit, el mal reputacional podria ser irreparable afectant no sols la seva imatge personal, sinó també els seus contractes de patrocini i la confiança dels aficionats així com allò aconseguit en els seus clubs i la reputació d'aquests (FC Barcelona, Paris Saint Germain, Inter Miami i AFA). L'abundància de dades biomètriques disponibles sobre esportistes (imatges de partits, entrevistes, xarxes socials) els fa especialment vulnerables i els posa en major situació de risc de ser víctimes de vulneracions, contribuint a la vegada això a un escenari on els usuaris de les xarxes socials es tornen encara menys confiats en les notícies que troben en línia i poden arribar a ser menys propensos a comportar-se de manera col·laborativa i responsable amb altres usuaris quan comparteixen les mateixes notícies.

A llarg termini, l'expectativa general que poc del que està disponible en línia pot ser de confiança pot contribuir encara més a una espiral actitudinal que “qualsevol cosa és vàlida (*anything goes*)” en línia. Això pot contribuir aleshores a disminuir el sentit de responsabilitat dels individus per la informació que comparteixen. També pot portar a la ciutadania a escapar de les notícies per evitar l'estrès derivat de la incertesa.³ Aquest aspecte planteja una qüestió sobre si és ètic que les figures públiques i, en aquest cas, els esportistes, suportin una vulnerabilitat desproporcionada per la seva visibilitat.

Una de les primeres formes més comunes de *deepfakes* és l'alteració de la pornografia, que representa individus no consensuats que participen en un acte sexual que mai es va produir típicament col·locant la cara d'una persona en el cos d'una altra persona. Donat el poder del sistema visual en alterar les nostres creences ja descrites, i la influència que aquests *deepfakes* poden tenir en la pròpia identitat, l'impacte en la vida d'una víctima pot ser devastador. Encara que la investigació empírica fins avui és limitada, no és difícil imaginar com es podrien utilitzar els *deepfakes* per extorsionar, humiliar o assetjar les víctimes.⁴

³ VACCARI, C., & CHADWICK, A. (2020). “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News.” *Social Media + Society*, 6(1). <https://doi.org/10.1177/2056305120903408>

⁴ HANCOCK, J. T., & BAILENSEN, J. N. (2021). *The social impact of deepfakes*. Virtual Human Interaction Lab, Stanford University.. pp. 150-151 <https://vhil.stanford.edu/publications/social-interaction/social-impact-deepfakes>

La manipulació de la imatge i veu de figures públiques afecta la confiança, la percepció pública i el benestar emocional. La investigació sobre el robatori d'identitat i el mal ús de deepfake suggereix que les víctimes de deepfakes sobre les quals s'utilitza sense el seu consentiment pot conduir a l'ansietat, l'estrès i els sentiments d'impotència i violació.⁵ Aquesta ansietat i pèrdua de confiança pot resultar en un impacte especialment greu en esportistes la carrera dels quals depèn de la seva imatge pública i estabilitat emocional. Per exemple, un tennista enfrontat a un *deepfake* que el mostri en una situació comprometedora podria veure afectada la seva concentració en tornejos clau, la qual cosa remarca especialment la necessitat d'abordar aquestes qüestions des d'un enfocament ètic integral.

Finalment, la IA generativa planteja un desafiament a la veracitat en l'esport, fet que ja s'ha enunciat prèviament sobre l'impacte d'aquests continguts a les xarxes socials i la desconfiança que genera en el públic. La recerca en *deepfakes* mostra que les opinions de les persones poden influir per les interaccions amb una rèplica digital, fins i tot quan saben que no és la persona real. Això pot crear records "falsos" d'algú. Els falsos records negatius podrien danyar la reputació de la persona retratada. Els falsos records positius també poden tenir efectes interpersonals complicats i inesperats.⁶

La proliferació de contingut fals pot erosionar per tant la confiança dels aficionats en les declaracions i accions dels atletes, un pilar fonamental de l'ecosistema esportiu. Aquest dilema ètic transcendeix l'individual per a afectar també la col·lectivitat exigint una reflexió profunda sobre els límits de la tecnologia i el seu impacte en la integritat de l'esport com a institució social.

⁵ Marlynn Wei M.D., J.D. (Actualitzat a 13/02/2024 i consultat 30/03/2025). *The Psychological Effects of AI Clones and Deepfakes. Concerns range from misuse to the potential impact on reputation and identity.* Psychology Today
<https://www.psychologytoday.com/us/blog/urban-survival/202401/the-psychological-effects-of-ai-clones-and-deepfakes>

⁶ Op cit 4

2.2 - Usos i límits de la IA en els drets de la personalitat: delimitació entre *deepfakes* i contingut identificat

La IA generativa brinda un ampli ventall de possibilitats en l'àmbit esportiu, des de la recreació de jugades històriques fins a la producció de contingut promocional o humorístic. La clau per a determinar la seva licitud radica en la distinció entre els *deepfakes* i el contingut generat per IA identificat com a tal. Segons l'article 3(60) de l'AI Act (Reglament 2024/1689)⁷, un *deepfake* és un "un contingut d'imatge, àudio o vídeo generat o manipulat per una IA que s'assembla a persones, objectes, llocs, entitats o successos reals i que pot induir a una persona a pensar erròniament que són autèntics o verídics;", la qual cosa implica una intenció d'engany en ometre la seva naturalesa artificial. Aquest mateix Reglament AI Act no els prohibeix per complet com calia esperar, i en el seu lloc ha decidit exigir que els creadors d'IA actuïn en general de manera transparent. Segons aquest marc, qualsevol que creï o utilitzi un *deepfake* ha de revelar el seu origen artificial i proporcionar informació sobre les tècniques utilitzades.

En aquest sentit, l'AI Act aborda el «problema dels *deepfakes*» a través de tres elements clau: (1) la definició de «*deepfake*»; (2) les obligacions de transparència per als proveïdors d'IA i els qui la utilitzen, també coneguts com a creadors de *deepfakes*; i (3) els objectius establerts en els considerants 132 a 137.

L'AI Act classifica els *deepfakes* en funció del seu risc potencial (risc inacceptable, alt, limitat i mínim), imposant normes més estrictes per als riscos més elevats. Les falsificacions profundes solen classificar-se en la categoria de risc limitat.

El «risc limitat» es refereix als riscos associats a la falta de transparència en l'ús de la IA. L'article 50 del Reglament introdueix obligacions específiques de transparència per garantir que s'informa els humans, quan sigui necessari, l'objectiu del qual és fomentar la confiança. Per exemple, a l'hora d'utilitzar sistemes d'IA com els *bots*, els humans han de saber que estan interactuant amb una màquina perquè puguin prendre una decisió informada de continuar o retrocedir. Els proveïdors també hauran de garantir que els continguts generats

⁷ UE. (2024). Reglament (UE) 2024/1689 del Parlament Europeu i del Consell de 13 de juny de 2024 per el que s'estableixen normes armonitzades en matèria d'intel·ligència artificial i per el que es modifiquen els Reglaments (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 i les Directives 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Reglament d'Intel·ligència Artificial). DOUE, L 1689, 12.7.2024.

<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689>

per IA siguin identificables, i que el text generat per IA que es publiqui amb el propòsit d'informar el públic sobre assumptes d'interès públic s'etiqueti com generat artificialment. Això també s'aplica als continguts d'àudio i vídeo que constitueixin falsificacions profundes.

El considerant (134) subratlla el punt (2) anterior i la importància de les obligacions de transparència previstes a l'article 50, anticipant que ha d'exigir-se als qui despleguin sistemes d'IA que revelin clarament que el contingut ha estat creat o manipulat artificialment, etiquetant el resultat de la IA en conseqüència i revelant el seu origen artificial.

Encara que la inclusió «per defecte» dels *deepfakes* en la categoria de risc limitat és certament discutible tenint en compte el mal que són capaços de causar, la bona notícia és que la Llei d'IA també preveu la possibilitat teòrica que els *deepfakes* puguin entrar en la «categoria d'alt risc» degut al potencial de manipulació de continguts polítics o electorals⁸.

D'altra banda, un escenari diferent apareix quan un vídeo etiquetat com generat per IA, per exemple, una paròdia d'un futbolista cantant o parlant amb un company en to humorístic, no es considera *deepfake* ja que la seva transparència elimina el component il·lícit. És aquest el component que implica que el material audiovisual que podria ser etiquetat com a *deepfake* no sigui valorat com a tal, doncs la transparència i la claredat per identificar de forma distintiva que el contingut multimèdia que està consumint l'usuari hagi estat generat via IA implica que no s'està perseguint un engany, no es té per objectiu induir una persona a pensar que allò que se li mostra és verídic.

Per la seva pròpia definició i essència, el significat i objectiu intrínsec d'un *deepfake* és el frau, difamació, desinformació i engany. Això ens planteja si és protegible el *deepfake*? Una obra o vídeo és protegible via dret d'autor i propietat intel·lectual, però quan ho califiquem com a *deepfake* ja no, doncs es tracta d'una creació contrària a la llei sobre l'ús d'IA. No es pot utilitzar el monopoli del dret d'autor per acollir dins d'aquest dret tota creació de *deepfakes*; es pot protegir un vídeo però no si aquest es tracta d'un *deepfake*. El vídeo, si vulnera el dret a la pròpia imatge i la veu d'algú sense el seu consentiment, ja no és protegible.

⁸ JACOBACCI, EUGENIO. (20/09/2024). *AI and Deepfakes: EU and Italian Regulations*. Legal500. <https://www.jacobacci.com/en/publications/ai-and-deepfakes>

Hi ha una vulneració de dades personals si s'utilitzen dades biomètriques (definides a l'article 4 GDPR⁹) per a l'elaboració d'aquest contingut, contingut il·lícit. S'ha de tenir també en compte que, si el *deepfake* es basa en dues fotografies o obres previes per fer-ne una de nova, es vulnera el dret d'autor pel fet de ser en si mateix un engany que utilitza aquesta base, es tracta d'un ús indegut no només del dret de la personalitat sinó també d'obres preexistents.

L'explotació comercial del contingut il·lícit donarà lloc a la responsabilitat civil, administrativa i penal.

Posem per exemple una plataforma o xarxa social que permet la difusió del *deepfake* d'un esportista. Aquestes plataformes poden ser responsables subsidiaris i han de detectar i retirar aquests continguts maliciosos. Si ens trobem amb un *deepfake* però la finalitat és lícita, aquest material requerirà ser identificat com a generat via IA i el clar consentiment de la persona de la qual es repliquen dades biomètriques, però si l'ànim és enganyar i no està identificat com a generat per IA ja no serà un material lícit i la persona que ha prestat consentiment en serà també responsable. En resum, si hi ha consentiment però es tracta de material no identificat i es busca l'engany es tracta per tant d'un *deepfake* i l'ús encara és il·lícit per definició.

La conclusió jurídica del *deepfake* és que aquest és il·lícit per naturalesa, quan és lícit es tracta de paròdia i és protegible per dret d'autor i no se'l classifica com a *deepfake* per molt que la tecnologia emprada sigui la mateixa. Una falsificació profunda no és en essència mai lícita, tot el que és fals és punible.

Aquesta delimitació té profundes implicacions ètiques i legals. L'ús identificat de la IA respecta el principi de veracitat, en informar el públic del seu origen artificial, i no busca danyar la reputació de l'esportista. Per exemple, un club podria emprar IA per a recrear un gol icònic d'un exjugador amb finalitats nostàlgiques i d'interaccions a les xarxes socials, sempre que s'indiqui el seu caràcter de generat artificialment. Un escenari contrari seria un *deepfake* que simuli un atleta promocionant un producte fraudulent, aquest material sense l'etiqueta de "generat artificialment" vulnera la confiança pública i la integritat personal, constituint un acte legal i èticament reprovable.

⁹ UE. (2016). *Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i per el que es deroga la Directiva 95/46/CE*. EUR-Lex. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>

Per al contingut generat via IA generativa s'aplicarà el límit que la paròdia estableix als drets d'autor, no sent necessari recaptar autorització dels personatges públics per a l'ús de la seva imatge. No obstant l'anterior, és important saber que en cap cas està permès que a través de la paròdia s'arribi a l'insult. La paròdia es realitza i s'ha de percebre exclusivament amb una finalitat humorística, i deixa de ser-ho quan a través del *deepfake* s'insulta o menysprea als personatges que en ella apareixen.

Per tant, l'ús de la tecnologia *deepfake* encara que en determinades ocasions pot entrar en col·lisió amb els drets d'imatge, és lícit si es compleixen determinats requisits que resumim a continuació:

- Quan l'ús de la tecnologia *deepfake* té una finalitat comercial és necessari recaptar l'autorització expressa de tots aquells que apareixen en el vídeo i, si hagués mort, acudir als hereus o descendents directes per a obtenir aquest consentiment.
- No és necessari el consentiment d'aquells personatges que exerceixin un càrrec públic o una professió de notorietat o projecció pública quan la finalitat del vídeo és exclusivament humorística i compleix amb els requisits necessaris per a ser qualificat com a paròdia.¹⁰

Jurídicament, aquesta distinció es reflecteix en diverses normes.

2.3 - Règim legal europeu aplicable a l'ús d'IA en l'esport

Dins del marc normatiu europeu, aquest proporciona un conjunt d'eines per la protecció dels drets d'imatge i veu de figures públiques, dins dels quals trobem els esportistes, amb la particularitat que la seva condició professional els aporta tant fortaleeses com limitacions.

Una de les normes clau en aquest camp és el Reglament General de Protecció de Dades (GDPR, Reglament 2016/679)¹¹, el qual estableix en el seu article 4. 14) què es considera per

¹⁰ PÉREZ-CABRERO, ISABEL. (09/02/2021). *Los 'deepfakes' y su relación con los derechos de imagen: ¿cuál es el límite?* Blog Propiedad Intelectual e Industrial Garrigues <https://blogip.garrigues.com/propiedad-intelectual/los-deepfakes-y-su-relacion-con-los-derechos-de-imagen-cual-es-el-limite>

¹¹ Op. cit 8

dades biomètriques, com la imatge i la veu, que són dades personals sensibles, el tractament de les quals està subjecte a condicions estrictes (art. 9 del mateix Reglament). L'ús no autoritzat d'aquestes dades, les quals són indispensables per a la creació de contingut identificable com a *deepfakes* constitueix una infracció dels principis de licitud, lleialtat i transparència establerts a l'art. 5.1, podent implicar sancions de fins a 20 milions d'euros o el 4% de la facturació anual global d'acord amb el que estableix l'art. 83.5 a). Cal considerar també l'article 22, el qual estableix per a tot interessat, esportistes inclosos per tant, el dret a no ser objecte de decisions automatitzades que els afectin significativament, la qual cosa podria invocar-se si un *deepfake* danya la seva carrera o reputació.

És especialment rellevant el concepte de privacitat amb el del dret a la imatge i quina protecció rep. El cas *Reklos i Davourlis v. Grècia*¹² va reconèixer el dret a la imatge com a part de la privacitat sota l'Article 8 del CEDH, establint un precedent per a contextos digitals. Aquest fet proporciona a les figures públiques esportives un context idoni per la protecció de la seva privacitat i per tant, de la no difusió d'imatges de la seva persona, incloent-hi les generades via *deepfake*.

Aquest enfocament basat en la protecció de dades resulta especialment rellevant en l'esport, ja que els atletes són figures públiques amb una exposició massiva de les seves dades biomètriques en esdeveniments i xarxes socials.

Un altre dels actors principals en la regulació aplicable a aquest treball és la Llei d'Intel·ligència Artificial (AI Act, Reglament 2024/1689), de 13 de juny de 2024. L'AI Act busca equilibrar la innovació tecnològica amb la protecció de drets fonamentals, un objectiu que va en concordança amb els desafiaments de l'esport. Aquesta norma introdueix un marc específic per regular els sistemes d'IA, dins dels quals s'inclouen els *deepfakes*. Aquesta norma classifica els diferents tipus de sistemes d'IA en diferents graus de risc: inacceptable, alt, limitat o específic i baix o mínim. Els *deepfakes* subjecte d'anàlisi d'aquest treball es troben classificats dins la categoria de sistemes d'IA de risc limitat o específic, els quals exigeixen una especial èmfasi en els principis i obligacions de transparència i informació. Aquestes obligacions de transparència van dirigides a dos tipus de subjectes: els proveïdors de sistemes d'IA (persones físiques o jurídiques que desenvolupin un sistema o model d'IA) i

¹² TEDH. (15/04/2009). *Case of Reklos and Davourlis v. Greece* (application no. 1234/05) HUDOC . <https://hudoc.echr.coe.int/eng?i=001-90617>

els responsables del desplegament (persones físiques o jurídiques que utilitzin un sistema d'IA sota la seva pròpia autoritat).

Respecte als primers, s'estableix que han de vetllar perquè els resultats de sortida del sistema d'IA estiguin marcats en un format llegible per màquina i que sigui possible detectar que han estat generats o manipulats de manera artificial (art. 50.2). Aquesta obligació no s'aplicarà si els sistemes d'IA es limiten a donar suport a l'edició estàndard o no alteren substancialment les dades d'entrada o quan estiguin autoritzats per la llei.

Pel que fa als responsables del desplegament d'un sistema d'IA, han de fer públic que aquests continguts o imatges han estat generats o manipulats de manera artificial (art. 50.4), és a dir, han de portar com una “marca d'aigua” que adverteixi que són generats amb tecnologia *deepfake*. Si el contingut és part d'una obra creativa, satírica o similar, aquesta obligació es limitarà a advertir que es tracta d'un contingut generat o manipulat artificialment de manera que no dificulti l'exhibició o gaudi de l'obra.¹³

Considerant l'article 6 de l'AI Act, aquest no podria considerar els *deepfakes* esportius com a sistemes d'alt risc tret que portin a la desinformació massiva, un fet difícilment possible però encara més difícilment valorable degut a interpretacions subjectives. Posem per exemple, un muntatge *deepfake* que afecti al conegut “Cas Negreira”, que podria portar a un dany reputacional irreparable sobre una falsa “compra” d'àrbitres per part del FC Barcelona. Es tracta d'un club amb impacte mundial, amb milions de seguidors i un impacte en els valors i la ètica de l'esport que reben les persones i l'ecosistema que conformen. L'impacte comercial i en aquests valors podria considerar-se una afectació per desinformació massiva? Aquest criteri de la desinformació massiva limita l'abast dels *deepfakes* d'esportistes d'èlit a casos de danys més aviat individuals. A més, les federacions esportives internacionals, com la FIFA, UEFA o el COI, no compten amb normatives específiques sobre IA, deixant la protecció dels atletes en mans de les lleis generals i generant possibles llacunes legals.

El passat 11 de març de 2025 el Consell de Ministres va aprovar l'Avantprojecte de Llei per al bon ús i la governança de la Intel·ligència Artificial (“Avantprojecte de Llei d'IA”)¹⁴, que

¹³ ANSÓN PEIRONCELY, RAFAEL. (12/11/2024) *La regulación de los Deep Fakes. ¿Se pueden poner puertas al campo?* Blog Bufete Mas y Calvet
<https://mascalvet.com/la-regulacion-de-los-deep-fakes-se-pueden-poner-puertas-al-campo/>

¹⁴ Gobierno de España, Secretaría de Estado de Digitalización e Inteligencia Artificial y Telecomunicaciones. (Març 2025.). *Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial*. Ministerio para

desenvolupa el règim sancionador i de governança previst en el Reglament (UE) 2024/1689 *AI Act*. Aquest desenvolupa el règim sancionador i de governança de l'AI Act conforme al seu art. 99. En particular, estableix una classificació de les infraccions en lleus, greus o molt greus, associant en cada cas les pertinents sancions que concreta el propi text. En les infraccions molt greus per pràctiques d'IA prohibides i en les infraccions en què un sistema d'IA hagi causat un incident greu, l'autoritat de vigilància del mercat podrà imposar la retirada del producte o la desconnexió o prohibició del sistema d'IA. L'article 34 de l'Avantprojecte assigna a l'infractor l'obligació de reposició a l'estat originari de la situació que s'hagi alterat més les corresponents penes i indemnitzacions de danys i perjudicis que hagi provocat.

D'acord amb l'Art. 50 del Reglament d'IA, l'art. 16 de l'Avantprojecte tipifica com a infracció greu per als proveïdors de sistemes d'IA l'incompliment de l'obligació d'etiquetar correctament qualsevol imatge, àudio o vídeo generat o manipulat amb IA que constitueixi una ultrasuplantació (*deepfake*) o qualsevol text destinat a informar el públic sobre assumptes d'interès públic, així com l'incompliment de l'obligació d'informar les persones afectades sobre el fet que estan interactuant amb un sistema d'IA. Els continguts indicats hauran d'identificar-se com a continguts generats per IA “de manera clara i distingible a tot tardar en ocasió de la primera interacció o exposició”.¹⁵

L'art. 6 de l'Avantprojecte designa les autoritats de vigilància del mercat competents per a l'exercici de la potestat sancionadora.

En relació amb aquesta norma trobem l'Agència Espanyola de Supervisió d'Intel·ligència Artificial (AESIA), estatuts de la qual foren publicats a través del Reial Decret 729/2023, de 22 d'agost.¹⁶ Aquesta actua com a garant de supervisar el compliment de l'Avantprojecte en sectors específics, inclòs l'esportiu, on la imatge dels atletes és un actiu econòmic vulnerable i, com a titular de la potestat sancionadora en relació amb la majoria de les pràctiques

la transformación digital y de la función pública.

https://avance.digital.gob.es/_layouts/15/HttpHandlerParticipacionPublicaAnexos.ashx?k=19128

¹⁵ TENA, PABLO I SALA, MIREIA. (26/03/2025). *Anteproyecto de Ley para el buen uso y gobernanza de la IA*. Blog de Propiedad Intelectual y Tecnologías Cuatrecasas.

<https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/anteproyecto-ley-buen-uso-gobernanza-ia>

¹⁶ Gobierno de España. (2023). Reial Decret 729/2023, de 27 d'agost, per el qual s'aprova l'Estatut de l'Agència Espanyola de Supervisió d'Intel·ligència Artificial. BOE, núm. 210, 2 de setembre de 2023, pp. 122289-122316.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-18911

prohibides, així com de bona part dels sistemes d'alt risc de l'Annex III del Reglament IA, i amb les obligacions de transparència de determinats sistemes. Aquest avantprojecte reforça la protecció enfront de *deepfakes* a Espanya, oferint un marc nacional més detallat que podria aplicar-se a casos com per exemple la difusió d'un vídeo fals d'un jugador de *LaLiga* promocionant apostes il·legals.

A nivell nacional, la Llei orgànica 1/1982, de 5 de maig, protegeix el dret a l'honor, la intimitat i la pròpia imatge¹⁷. El seu article 7.5 qualifica com a intromissió il·legítima l'"ús de la imatge o veu d'una persona captada en un lloc públic o privat sense el seu consentiment", la qual cosa s'aplica als *deepfakes*. Per exemple, un tribunal espanyol podria ordenar la retirada d'un *deepfake* esportiu i concedir indemnitzacions per danys morals com ve indicat a l'art. 9.3. No obstant això, la falta de jurisprudència específica sobre IA en l'esport limita la predictibilitat d'aquestes respostes legals.

L'article 11 de la Llei de Competència Deslleial (Llei 3/1991) a Espanya prohibeix els actes d'imitació que generin confusió o aprofitin indegudament la reputació aliena, la qual cosa podria aplicar-se a *deepfakes* comercials no autoritzats en l'esport. Per exemple, un anunci fals d'un esportista promocionant apostes il·legals sense el seu consentiment seria sancionable sota aquesta norma, ja que explota la seva imatge de marca de manera deslleial.

L'article 8 del Conveni Europeu de Drets Humans (CEDH) complementa aquest marc, garantint el respecte a la vida privada. El TEDH, al *cas Peck v. el Regne Unit* (2003, Application no. 44647/98)¹⁸, va reconèixer que la difusió no autoritzada d'imatges vulnera aquest dret, un precedent aplicable a *deepfakes* esportius. No obstant això, la menor expectativa de privacitat dels esportistes com a figures públiques que s'estableix a l'*assumpte Von Hannover v. Alemanya* (No.2) (2004, Applications nos. 40660/08 and 60641/08)¹⁹, complica el seu defensa enfront d'usos satírics o comercials, generant una tensió amb la llibertat d'expressió (art. 10 CEDH).

¹⁷ 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. (1982). BOE, num. 115, pp. 12546-12548.
<https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196>

¹⁸ TEDH. (28/01/2003) *Peck v. the United Kingdom*, Application No. 44647/98 (2003).
<https://hudoc.echr.coe.int/eng?i=001-60898>

¹⁹ TEDH. (07/02/2012). *STS Asunto Von Hannover c. Alemania (no 2)*, Demandas nos 40660/08 et 60641/08).
<https://hudoc.echr.coe.int/eng?i=001-139414>

Tot aquest règim normatiu, encara que robust i complementat per varies lleis, presenta llacunes. L'absència d'una regulació específica en el dret esportiu nacional i internacional juntament amb la dificultat de perseguir *deepfakes* creats fora de la jurisdicció de la UE evidencien la necessitat d'una harmonització més efectiva, un repte que l'Avantprojecte de Llei d'IA espanyol intenta abordar a nivell nacional, però que requereix coordinació supranacional.

2.4 - Casos d'usos i vulneracions de drets de la personalitat d'esportistes a través de *deepfakes*

L'ús de *deepfakes* ha vulnerat en ocasions els drets de la personalitat d'esportistes, evidenciant les tensions entre la intel·ligència artificial generativa i els marcs normatius aplicables. Aquest subapartat analitza casos reals que il·lustren les repercussions jurídiques i ètiques d'aquestes manipulacions, destacant-ne el cas de Lionel Messi i altres exemples documentats que afecten figures públiques, amb especial atenció a l'impacte que una vulneració d'aquest tipus pot generar a l'àmbit esportiu. S'examinen les normes infringides i les responsabilitats derivades, subratllant la il·licitud intrínseca dels *deepfakes* enfront de continguts lícits identificats com generats per IA.

El cas més il·lustratiu per la dimensió de la figura dins del món de l'esport que es tractarà en aquest estudi és el de Lionel Messi, víctima l'any 2023 d'un *deepfake* difós en plataformes com Instagram o YouTube, que el mostrava promocionant l'aplicació d'apostes "*Wildcat Dive*". El vídeo, creat sense el seu consentiment, el presentava afirmant que aquesta aplicació era una font clau d'ingressos per a ell destacant que es tracta d'una inversió segura i que l'aplicació havia beneficiat a milers de persones, amb la finalitat d'enganyar usuaris per a obtenir beneficis econòmics il·lícits. "*Si tenés 75.000 pesos en una semana se convierten en 2 millones de pesos. No necesítas ser un experto en economia ni en mercados*", expressa el suposat Messi amb la seva característica veu i accent argentí juntament amb la seva imatge.

Aquest contingut utilitza fragments d'una entrevista real que el futbolista va concedir fa alguns mesos al programa argentí de *streaming*, "Olga". En el vídeo alterat, tant la veu de l'entrevistador com la del futbolista han estat artificialment modificades per a fer creure als espectadors que estan presenciant una promoció genuïna de l'aplicació. A més, els estafadors

utilitzen dues estratègies més per a enfortir aquesta falsa creença: En primer lloc, el futbolista esmenta altres fonts d'ingrés com a contractes publicitaris amb reconegudes marques, la qual cosa és cert. En segon lloc, es mostren vídeos de publicitats mentre el futbolista parla, per a evitar que l'usuari pugui notar les diferències entre la veu i el moviment dels llavis de les persones involucrades i així detectar l'estafa.²⁰

La notícia sobre aquest *deepfake* va començar a circular per xarxes socials després que el periodista Maximiliano Firtman expliqués que a un conegut seu li va aparèixer la història on Messi publicitava la plataforma.

"Hi ha molt d'això", va remarcar l'expert en estafes en diàleg amb l'Agència Notícies Argentines, i això s'emmarca en les desenes de vegades que l'astre del futbol va ser víctima d'enganyoses publicitats amb la seva cara.

A més, la divulgació d'aquest vídeo provoca que centenars de persones caiguin en el parany de l'esquema Ponzi, el qual sempre finalitza en una estafa piramidal.²¹

Dins del món esportiu del futbol trobem un altre cas rellevant d'ús de tecnologia *deepfake* en la figura del seleccionador de l'equip nacional de futbol d'Anglaterra, Gareth Southgate. Al juny de 2024, durant el torneig de l'Eurocopa 2024 organitzat per la Unió d'Associacions Europees de Futbol (UEFA), van circular vídeos en plataformes com TikTok i Instagram mostrant a Gareth Southgate fent comentaris grollers i ofensius sobre jugadors com Phil Foden, Jordan Henderson, Jack Grealish i Marcus Rashford²². Aquests vídeos, generats mitjançant IA, simulaven conferències de premsa i utilitzaven una veu artificial per a atribuir declaracions falses sobre els seus propis jugadors, la qual cosa va generar confusió entre alguns espectadors.

²⁰ LÓPEZ, MARTINA. (25/03/2024) *Alerta por deepfake de Lionel Messi para promover una aplicación fraudulenta* Newsletter welivesecurity. Noticias, opiniones y análisis de la comunidad de seguridad de ESET <https://www.welivesecurity.com/es/estafas-enganos/alerta-deepfake-messi-utilizado-promover-aplicacion-fraudulenta/>

²¹ DIARI ARGENTÍ ÀMBITO. (23/10/2024). *Lionel Messi sufrió una "deepfake": utilizaron una entrevista suya para promocionar una estafa piramidal* <https://www.ambito.com/deportes/lionel-messi-sufrio-una-deepfake-utilizaron-una-entrevista-suya-promocionar-una-estafa-piramidal-n6073788>

²² SCOTT, LAURA. (30/06/2024). *'Deepfake' Southgate videos viewed by millions*. BBC Sport. <https://www.bbc.com/sport/football/articles/cqqldv3qy1lo>

Un cas especialment rellevant per aquest treball és el cas *Eddie Irvine v. Talksport Ltd*²³, en aquest cas el pilot de Fórmula 1 Eddie Irvine va demandar a l'emissora *Talksport* per utilitzar una imatge manipulada seva en un anunci que suggeria el seu *endorsement*²⁴ de l'estació de ràdio sense el seu consentiment. El tribunal va determinar que l'ús constituïa *passing off*²⁵ (imitació fraudolenta) sota la llei anglesa, ja que induïa a error al públic sobre la relació d'Irvine amb *Talksport*. Irvine va rebre una indemnització per danys, establint un precedent per a la protecció dels drets d'imatge d'esportistes. Precisament per aquest últim punt, tot i no implicar l'ús de tecnologia *deepfake* ja que l'any 2002 aquesta no existia, aquest cas pot aportar una direcció del tractament que els tribunals podrien donar a les vulneracions d'imatge i veu sobre figures del món esportiu que es poden generar via IA.

Un altre cas recent a l'estat espanyol que podríem adaptar a l'esport, és el famós cas d'Almendralejo, on menors van ser víctimes de *deepfakes* pornogràfics creats a partir de fotos públiques. Encara que no va involucrar esportistes, l'incident, reportat per El País²⁶, és extrapolable a figures com futbolistes femenines (ja que l'immensa majoria de *deepfakes* pornogràfics tenen com a víctimes figures femenines) i fins i tot, esportistes menors, l'exposició mediàtica dels quals les fa vulnerables a manipulacions similars. Aquest *deepfake* va infringir l'article 197 del Codi Penal espanyol, que castiga la difusió no autoritzada de dades personals amb penes de fins a 4 anys de presó (Llei orgànica 10/1995). L'Avantprojecte de Llei per al bon ús i la governança de la IA classifica aquest acte com "ultrasuplantación" (art. 12), amb sancions de fins a 30.000 euros o presó en casos greus, reforçant la protecció enfront de l'ús il·lícit de dades biomètriques. L'impacte psicològic en les víctimes, el dany reputacional i a l'honor així com les conseqüències d'estrès, ansietat i altres afectacions com

²³ ENGLAND AND WALES HIGH COURT (CHANCERY DIVISION) DECISIONS. (13/03/2002). *Edmund Irvine Tidswell Ltd. v Talksport Ltd.* [2002] EWHC 367 (Ch) (13th March, 2002). BAILII Databases. <https://www.bailii.org/ew/cases/EWHC/Ch/2002/367.html>

²⁴ *Endorsement* és una activitat de màrqueting molt pròxima al patrocini. És una activitat creixent que duen a terme sobretot les marques de roba, empreses musicals i de l'espectacle. L'empresa contracta els serveis d'un artista, músic, o esportista d'elit per fer-lo servir de "maniquí en vida" dels seus productes. El contractat es compromet a portar productes d'aquesta marca en les situacions pactades en el contracte.

²⁵ EVANS, BEN.(13/10/2023). *What is passing off? Legal advice, defences and remedies*. Harper James. <https://harperjames.co.uk/article/passing-off/>

²⁶ RUIZ DE VALBUENA, IRENE. (19/09/2023. ACTUALIZADO:20/09/2023 - 10:24 CEST). *Caso Almendralejo: La difusión de las imágenes manipuladas de menores desnudas es también una infracción de protección de datos*. El País Madrid - 19/09/2023 - 14:42 https://elpais.com/economia/2023/09/19/mis_derechos/1695125490_270661.html

la pèrdua de confiança que poden afectar el rendiment esportiu i la qualitat de vida van de la mà amb els majors riscos que enfronten els esportistes.

Un exemple real més és el *deepfake* del polític italià Mario Draghi el passat 2023. En un vídeo fals se'l veu promocionant inversions fraudulentament convencent uns 45 italians que van veure el vídeo a Instagram per seguir “els seus” consells²⁷. El cas comparteix similituds amb el de Messi doncs tots dos afecten una figura pública mitjançant engany comercial. En el context esportiu, aquest precedent il·lustra com els *deepfakes* poden explotar la imatge d'atletes d'elit amb una reputació i credibilitat per a fins econòmics il·lícits, violant l'article 8 del Conveni Europeu de Drets Humans (CEDH). Aquestes manipulacions atempten contra la integritat col·lectiva del sector afectat, com l'esport²⁸.

Aquests casos reals fan paleses les vulneracions que els *deepfakes* provoquen en els drets d'imatge i veu dels esportistes en ometre el consentiment i la transparència exigits pel GDPR i l'AI Act.

L'explotació comercial il·lícita genera responsabilitats civils contractuals, administratives i penals sota normes nacionals i internacionals, mentre que èticament comprometen la confiança pública i el benestar dels afectats. La ràpida difusió en plataformes digitals, com en el cas de Messi, exigeix una resposta coordinada i harmonitzada de les normes legals.

3. Nous horitzons i reptes per als esportistes en l'era digital més enllà de les vulneracions per *deepfakes*

3.1 - Exposició pública amplificada i pressió social sobre els drets d'imatge i veu dels esportistes

La immensa visibilitat dels esportistes es deriva d'una banda de la seva presència constant en plataformes digitals i xarxes socials com ara Instagram, X o TikTok. Aquestes permeten als atletes compartir aspectes de la seva vida personal i professional, generant així un flux

²⁷ JACOBACCI AVVOCATI en col·laboració amb JACOBACCI & PARTNERS. (23/09/2024). *AI and Deepfakes: EU and Italian Regulations*. Article publicat a *Legal500*
<https://www.jacobacci-law.com/news-and-publications/ai-and-deepfakes-eu-and-italian-regulations>

²⁸ ROMERO MORENO, FELIPE. (29/03/2024). *Generative AI and deepfakes: a human rights approach to tackling harmful content*. *International Review of Law, Computers & Technology*, 38(3)297-326.
<https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2324540#d1e481>

continu de dades biomètriques accessibles globalment. Les retransmissions esportives, amb càmeres d'alta definició que capturen cada gest, i les bases de dades públiques com arxius d'imatges i vídeos amplifiquen aquesta exposició. Segons estudis, la recopilació de dades biomètriques en l'àmbit esportiu, inclosos patrons facials i vocals, ha crescut exponencialment a causa de la digitalització dels esdeveniments esportius²⁹.

Aquestes dades, definides a l'article 4 (14) del GDPR com aquelles que permeten la identificació única d'una persona, són especialment sensibles. La seva disponibilitat massiva crea un entorn propici per a usos no autoritzats, com la creació de *deepfakes* o l'explotació comercial sense consentiment, la qual cosa posa en risc els drets d'imatge i veu dels esportistes els quals es troben en una situació de vulnerabilitat desproporcionada degut a la seva major visibilitat.

El marc legal europeu proporciona eines per la protecció dels drets de privacitat dels esportistes, amb l'article 8 del Tribunal Europeu de Drets Humans (TEDH) com a pilar fonamental. Aquest article organitza la protecció d'aquests drets que en aquest treball es tracten garantint el dret al respecte de la vida privada i familiar, incloent-hi la protecció de la imatge i la veu com a elements essencials de la identitat personal. El TEDH ha interpretat aquest dret de manera àmplia, reconeixent que fins i tot les figures públiques (sent aquest punt d'especial interès doncs és el perfil dels esportistes amb major visibilitat i que més susceptibles són de veure usada la seva imatge de forma fraudolenta mitjançant tecnologia *deepfake*) tenen una esfera privada protegida.

En el cas *Von Hannover v. Alemanya*³⁰, el TEDH va determinar que la publicació de fotografies de la princesa Carolina de Mònaco en contextos privats, sense contribuir a un debat d'interès general, constituïa una violació de l'article 8 CEDH. En la mateixa direcció es va pronunciar també el TEDH en els Considerants 66 a 73 del *Cas Glukhin v. Russia (application no. 11519/20)*³¹ destacant que el processament de dades biomètriques, com imatges facials, requereix estrictes salvaguardes legals per evitar interferències

²⁹ PARK, JENNIFER. (17/02/2024). *Biometric Data Collection in Professional Sports Reveals Holes in Privacy Law*. The Columbia Journal of Law & the Arts. <https://journals.library.columbia.edu/index.php/lawandarts/announcement/view/685>

³⁰ Op cit 10

³¹ TEDH. (2023). *Cas Glukhin v. Russia (application no. 11519/20)*. Hudoc. <https://hudoc.echr.coe.int/eng?i=001-225655>

desproporcionades. Encara que no cita el GDPR directament, el cas és rellevant per l'àmbit esportiu, ja que els esportistes, a causa de la seva alta exposició, són vulnerables a tecnologies similars que podrien usar-se per a crear *deepfakes*.

Aquest precedent estableix per tant que els esportistes, encara que siguin figures públiques, poden reclamar protecció contra l'ús no autoritzat de les seves dades biomètriques, sempre que aquest ús no estigui justificat per un interès públic legítim.

Complementàriament, a nivell europeu el GDPR reforça aquesta protecció al classificar les dades biomètriques com a categoria especial de dades personals sota l'article 9, prohibint-ne el seu tractament excepte en casos específics, com el consentiment explícit o la necessitat per a protegir interessos vitals. L'article 5 del GDPR estableix principis fonamentals, com la licitud, la transparència i la minimització de dades, que obliguen a les plataformes digitals, clubs esportius i organitzadors d'esdeveniments a implementar mesures tècniques i organitzatives adequades per la protecció d'aquestes dades. El següent, l'article 6, exposa el requeriment del consentiment de l'interessat o una altra base sòlida legítima per tal que hi hagi un tractament lícit de les dades. La falta de compliment pot derivar en sancions significatives indicades a l'article 83.5 a) del mateix cos legal. En el context esportiu, on les dades biomètriques es recopilen massivament durant partits, entrevistes i publicacions en xarxes socials, aquestes normes són essencials per garantir que els drets dels esportistes siguin respectats.

La hipervisibilitat no només facilita vulneracions tècniques, com la creació de *deepfakes*, sinó que també intensifica la pressió social sobre els esportistes, exacerbant els danys a la seva integritat personal fins i tot abans que es generi una violació concreta. En l'entorn digital, la percepció pública pot ser manipulada ràpidament mitjançant rumors, desinformació o continguts virals en xarxes socials, la qual cosa pot erosionar la confiança dels aficionats, patrocinadors i mitjans de comunicació. Per exemple, un rumor infundat sobre un esportista, amplificat en plataformes com X o Instagram pot generar una percepció negativa que afecti contractes comercials o l'estabilitat emocional de l'atleta, fins i tot si se'n demostra la falsedat³². És precisament a les xarxes on entra en joc el filtratge d'aquestes dades i la responsabilitat de les plataformes. En aquest sentit trobem la sentència del TJUE *Fashion ID*

³² SOURAV, SUBHAM. (11/05/2024). *Social Media and Athlete Privacy: Navigating Legal Boundaries*. Global Sports Policy Review.

<https://www.g-spr.com/post/social-media-and-athlete-privacy-navigating-legal-boundaries>

GmbH & Co. KG v. Verbraucherzentrale NRW eV, C-40/17 29 de juliol de 2019³³, on el Tribunal va determinar que els operadors de llocs web que integren complements de xarxes socials, com el botó “M'agrada” de *Facebook*, són corresponsables del processament de dades personals, incloent-hi imatges de perfil, sota l'article 26 del GDPR. En aquest cas, una empresa alemanya va ser demandada per recopilar dades sense consentiment explícit. La sentència va destacar que el processament de dades visuals en plataformes digitals requereix transparència i consentiment, conforme als articles 5 i 6 del GDPR.

Encara que aquesta sentència no aborda IA explícitament, el cas és rellevant per a la difusió d'imatges d'esportistes en xarxes socials, on els *deepfakes* poden proliferar, i reforça la responsabilitat de les plataformes digitals.

Aquesta pressió social té un impacte significatiu en la salut mental i el rendiment esportiu. L'exposició constant a la vigilància pública, els comentaris negatius i l'expectativa de perfecció generen estrès, ansietat i, en casos extrems, trastorns psicològics que poden comprometre la carrera d'un atleta. La recerca suggereix que els esportistes, a causa de la seva alta visibilitat, són particularment vulnerables a aquestes dinàmiques, la qual cosa subratlla la necessitat d'un enfocament preventiu que abordi la pressió social com un factor de risc estructural. Protegir la integritat personal requereix crear un entorn on la privacitat dels esportistes sigui respectada des de l'inici, mitigant els efectes de la percepció pública abans que es tradueixin en danys irreparables.

La recopilació de dades en esports està en auge, donant pas a una era de l'"atleta hiperquantificat", com un informe recent del gegant consultor Deloitte ho va descriure. Des de l'anàlisi de vídeo impulsada per IA fins a la biometria recollida per “*smartphones*” i “*wearables*”, quantitats cada vegada més grans de dades estan guiant el personal i les decisions estratègiques, impulsant la identificació de talent i aportant grans diners.

Però l'explosió de dades al voltant dels cossos i la salut dels esportistes està plantejant qüestions ètiques i legals. El més important: qui posseeix totes aquestes dades, i com les utilitzaran per millorar, fer les coses més ràpid i qui es farà més ric?

³³ TJUE. (2019). *Sentència del Tribunal de Justícia (Sala Segona) de 29 de juliol de 2019 Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, C-40/17 29. Curia.

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=ES>

La Unió Europea ha fet més, però malgrat una empenta global per a la regulació de la privacitat, és poc probable que es posi fre a la revolució de les dades. L'única qüestió que queda és com s'utilitzen aquestes dades, qui les usa i si és a favor o en contra dels atletes.

“La veritable història aquí és la transformació de la societat, i l'esport, en punts de dades”, diu la bioètica Andy Miah, catedràtica de comunicació científica i futurs mitjans de comunicació a la Universitat de Salford al Regne Unit. "Els atletes gairebé deixen de ser humans, i es converteixen en una sèrie de punts de dades."

Dan Lorang, cap de rendiment de l'equip ciclista professional alemany BORA-hansgrohe, diu que part de l'educació d'un entrenador ha de ser com utilitzar aquesta informació en benefici de l'esportista. Tot i això, diu, “em puc imaginar que recollir massa dades es convertiria en un problema i que els atletes poden témer que la informació es pugui utilitzar contra ells.”

A causa de la històrica llei de privacitat GDPR, BORA-hansgrohe va haver d'abordar aquest repte amb cura. En el seu contracte amb els ciclistes, ara estipula que les dades d'entrenament s'han de retornar quan aquests abandonen l'equip. Les dades mèdiques, d'altra banda, són altament confidencials i normalment no són vistes per l'equip en absolut, llevat que "hi hagi alguna cosa que pugui afectar l'equip", diu Lorang³⁴.

3.2 - Limitacions tecnològiques i desafiaments de prevenció enfront de la manipulació de dades biomètriques

En el context de l'era digital, la manipulació de dades biomètriques, especialment a través de *deepfakes*, planteja un desafiament significatiu per a la protecció proactiva dels drets d'imatge i veu, particularment per als esportistes, els qui són figures públiques altament visibles. Aquest treball analitza les barreres tecnològiques que dificulten la implementació de sistemes efectius de detecció i autenticació de contingut generat per IA en temps real, considerant la ràpida viralització a les xarxes socials. S'examina com la falta de traçabilitat i l'evolució constant de les tecnologies basades en GANs desafien les obligacions de transparència establertes a l'AI Act, específicament en el seu article 50. L'enfocament és preventiu i tècnic,

³⁴ BUSCA, NICK. (02/02/2021). *As biometrics boom, who owns athletes' data? It depends on the sport.* The Washington Post <https://www.washingtonpost.com/sports/2021/02/02/athletes-biometrics-data-privacy/>

destacant les llacunes tecnològiques que afecten especialment els esportistes com a grup vulnerable.

Els *deepfakes* han aconseguit un nivell de sofisticació alarmant gràcies als avanços en tècniques d'aprenentatge profund, particularment les GANs. Aquestes xarxes, compostes per un generador que crea contingut i un discriminador que avalua la seva autenticitat, operen de manera adversativa per a produir resultats hiperrealistes. Models com *StyleGAN*, desenvolupat per Karras et al., i *DeepFaceLab* han demostrat la capacitat de generar imatges i vídeos d'alta resolució que imiten amb precisió dades biomètriques, com a rostres i veus d'esportistes³⁵.

Aquesta evolució tecnològica no tan sols facilita la creació de contingut maliciós, sinó que també posa en evidència les limitacions dels sistemes de detecció actuals, que depenen de la identificació d'artefactes visuals o inconsistències que es tornen cada vegada menys perceptibles. La detecció de *deepfakes* és un camp en constant desenvolupament, però enfronta múltiples obstacles tècnics. Els mètodes actuals, com els basats en xarxes neuronals convolucionals (CNN) o xarxes neuronals recurrents (RNN), busquen identificar anomalies com a moviments oculars inusuals, textures artificials o desajustaments en la il·luminació³⁶. No obstant això, a mesura que les GANs evolucionen, aquests desajustaments oculars, d'il·luminació etc... es minimitzen reduint l'eficàcia de les tècniques tradicionals de detecció. Segons Rossler et al., els *deepfakes* generats per models avançats presenten defectes gairebé imperceptibles, la qual cosa impulsa una “carrera armamentística” entre creadors i detectors³⁷.

La detecció en temps real, essencial per a contrarestar la viralització a les xarxes socials, és particularment problemàtica a causa de la necessitat de processar grans volums de dades amb baixa latència. A més, els models de detecció requereixen conjunts de dades etiquetades extenses i equilibrades, que són difícils d'obtenir a causa del ràpid sorgiment de nous tipus de

³⁵ KARRAS, TERO & LAINE, SAMULI & AILA, TIMO. (29/03/2019). *AStyle-Based Generator Architecture for Generative Adversarial Networks*. arXiv:1812.04948v3 [cs.NE] Cornell University, p 1-2
<https://arxiv.org/pdf/1812.04948>

³⁶Op cit 21, p 2-3

³⁷ RÖSSLER, ANDREAS & COZZOLINO, DAVIDE & VERDOLIVA, LUISA & RIESS, CHRISTIAN & THIES, JUSTUS & NIESSNER, MATTHIAS (26/08/2019) *FaceForensics++: Learning to Detect Manipulated Facial Images*. The Computer Vision Foundation, p 8
https://openaccess.thecvf.com/content_ICCV_2019/papers/Rossler_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images_ICCV_2019_paper.pdf

deepfakes. La falta de dades representatives i la desproporció entre contingut real i fals limiten la capacitat dels algorismes per generalitzar, augmentant el risc de falsos negatius en entorns dinàmics com les plataformes digitals. L'absència de mètodes fiables per a rastrejar l'origen del contingut generat per IA constitueix una barrera crítica per a la prevenció de la manipulació de dades biomètriques. Els *deepfakes* solen manca de “marques d'aigua” que indiquin la seva naturalesa artificial, la qual cosa dificulta la verificació d'autenticitat, especialment quan el contingut es comparteix a través de múltiples plataformes. La naturalesa descentralitzada d'Internet agreuja aquest problema, ja que el contingut pot ser alterat o replicat sense un registre clar de la seva procedència. Encara que tècniques com el *watermarking* o el registre en *blockchain*³⁸ han estat proposades per a millorar la traçabilitat, la seva implementació a gran escala enfronta desafiaments tècnics, com la necessitat d'estàndards universals i la resistència de plataformes no regulades a adoptar aquestes mesures³⁹.

3.3 Impacte i conseqüències econòmiques indirectes dels *deepfakes* en el valor de mercat dels esportistes

En l'àmbit de l'esport professional, la imatge i la veu d'un esportista no són només atributs personals, sinó actius econòmics fonamentals que constitueixen precisament el valor capital econòmic de la imatge de la persona que podem anomenar d'ara en endavant com “capital d'imatge”. Aquest capital és essencial per assegurar patrocinis i contractes i determina i té un gran impacte en el valor de mercat general de l'atleta. No obstant això, la tecnologia *deepfake*, utilitzant IA per generar contingut audiovisual hiperrealista, introdueix una incertesa significativa que amenaça aquest capital. La simple possibilitat que la imatge o la veu d'un esportista siguin manipulades sense autorització pot erosionar la confiança de patrocinadors i marques, reduint els ingressos potencials fins i tot sense que es produeixi una vulneració concreta.

³⁸ AEPD. (20/11/2020). *Blockchain (II): Conceptos básicos desde la protección de datos*. <https://www.aepd.es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos>

³⁹ L. FENG, W. ZHOU, W. LIU, Y. -S. ONG i K. C. TAN. (Maig 2022). *Solving Dynamic Multiobjective Problem via Autoencoding Evolutionary Search*. IEEE Transactions on Cybernetics, vol. 52, no. 5, pp. 2649-2662, <https://ieeexplore.ieee.org/document/9210737>

Aquest treball busca analitzar els efectes preventius i a llarg termini dels *deepfakes* en el mercat esportiu, centrant-se en la depreciació del “capital d’imatge” i la necessitat d’estratègies de gestió reputacional i protecció legal específica en l’àmbit esportiu per les característiques úniques d’aquest que s’han valorat anteriorment en aquest estudi.

Els *deepfakes* representen una amenaça indirecta al introduir incertesa sobre l'autenticitat de la imatge i la veu dels esportistes. Com es ve dient, un vídeo fals que mostri un atleta promocionant un producte fraudulent o fent declaracions controvertides pot generar confusió entre els consumidors i els patrocinadors, fins i tot si es demostra la seva falsedat. Aquesta desconfiança pot dissuadir a les marques d’invertir en atletes d’alta exposició, els qui depenen de la seva reputació i rendiment per assegurar contractes lucratius. El valor de la imatge d’un esportista és crucial en l’era dels *influencers*, on la percepció pública es tradueix directament en oportunitats econòmiques⁴⁰. Per exemple, la mera possibilitat que un *deepfake* pugui ser creat i difós pot portar als patrocinadors a exigir clàusules contractuals més estrictes o a reduir el valor dels acords, afectant els ingressos potencials de l’esportista.

La literatura acadèmica subratlla que els *deepfakes* poden infringir el dret a la publicitat, un component clau del valor de mercat dels atletes. En aquest sentit, el cas *Young v. NeoCortext, Inc. (2023)*⁴¹, encara que no involucra a un esportista i és el tractament jurisprudencial que ha donat l’Estat de Califòrnia i no pas un tribunal europeu, il·lustra com les aplicacions de *deepfake* poden violar els drets d’imatge, afectant la capacitat de les figures públiques (com podria ser la d’un esportista) per controlar el seu valor comercial⁴².

Aquest precedent suggereix que els esportistes podrien enfrontar pèrdues econòmiques similars si la seva imatge és explotada sense consentiment.

L’impacte econòmic dels *deepfakes* no es circumscriu únicament a l’esportista individual, sinó que s’estén als equips, federacions i marques esportives associades. La reputació d’un club o una lliga està intrínsecament lligada a la dels seus atletes més representatius i famosos, i un

⁴⁰BOWYER, WILLIAM. (12/05/2021) *Deepfakes in the world of entertainment and sport – A danger or a new opportunity?* Mackrell.Solicitors Blog. p 1-2.
<https://www.lexology.com/library/document.aspx?g=108a8fb5-7693-4cfc-8acb-5eb645d63a7e>

⁴¹UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA—WESTERN DIVISION. (04/03/2023). *Young v. NeoCortext, Inc.*, No. 2:23-cv-02496 (C.D. Cal. 2023).
<https://www.classaction.org/media/young-v-neocortext-inc.pdf>

⁴² BASS, DANIELLE F. & PENNING, NATHANIEL. (25/07/2023). *The Legal Issues Surrounding Deepfakes*. Honigman. <https://www.honigman.com/the-matrix/the-legal-issues-surrounding-deepfakes>

deepfake que comprometi la imatge d'un jugador pot repercutir en la percepció global de l'entitat. Per exemple, un *deepfake* que suggereixi un comportament indegut d'un atleta o d'altres més greus com podria ser dopar-se, podria reduir l'atractiu comercial de l'equip, afectant acords de patrocini col·lectiu o la venda de marxandatge. Aquest efecte subsidiari és particularment rellevant en un context on la confiança pública és essencial per al valor de mercat de les organitzacions esportives, com es destaca en un informe sobre els impactes econòmics dels *deepfakes*⁴³.

El cas *Eddie Irvine v. Talksport Ltd (2002)* és un precedent rellevant, encara que no involucra *deepfakes*. En aquest cas, l'ús no autoritzat de la imatge d'un esportista per a suggerir un *endorsement* comercial va ser resolt a favor del pilot de *F1* i considerat una infracció de *passing off*, causant pèrdues econòmiques. Aquest principi és aplicable als *deepfakes*, que poden generar danys similars en explotar la imatge d'un atleta per a fins comercials o difamatoris⁴⁴.

A llarg termini, els *deepfakes* poden generar una depreciaió general del "capital d'imatge" en l'ecosistema esportiu. L'amenaça constant de manipulació digital pot crear un efecte dissuasiu en el mercat de patrocinis, amb marques menys inclinades a invertir en atletes d'alta exposició. Això podria traduir-se en contractes menys lucratius, majors costos d'assegurança per tal de cobrir riscos reputacionals o la necessitat d'invertir en tecnologies de protecció digital. Per exemple, els esportistes podrien requerir sistemes d'autenticació basats en tecnologia *blockchain* per verificar l'autenticitat del seu contingut, la qual cosa incrementaria les seves despeses operatives.

A més, l'erosió de la confiança en el contingut digital esportiu pot afectar la comercialització de l'esport, reduint el valor dels contractes de patrocini en general. Un estudi de la *European Sponsorship Association* aquest últim any 2024 indica que fins al 20% de l'activitat de

⁴³ GITAN CHOPRA, GITAN & JOHAR, MANNAT KAUR. (18/06/2024). *The Economic Ripple Effect of Deepfake Disruption*. International Finance Student Association.
<https://ifsa-network.com/publications/the-economic-ripple-effect-of-deepfake-disruption/>

⁴⁴ Op cit 40

patrocini pot ser ineficaç si els consumidors no saben identificar contingut il·lícit o no confien en els missatges publicitaris, un risc que els *deepfakes* podrien agreujar⁴⁵.

La literatura també destaca que els *deepfakes* poden alterar la dinàmica dels fans esportius, afectant la percepció dels aficionats i, per tant, el valor comercial dels atletes. Una anàlisi d'un capítol de la obra *Black Communication in the Age of Disinformation* suggereix que els *deepfakes*, en introduir desinformació, poden socavar la confiança en les figures esportives, la qual cosa té implicacions econòmiques a llarg termini. Aquesta tecnologia canvia realment el paisatge de la comunicació i la celebritat esportiva. Degut a la profunda connexió dels aficionats amb els seus atletes esportius preferits, i aquests estan ara tan fàcilment a la disposició del públic, això fa que es generi una perillosa combinació en mans d'aquells que busquen estendre informació confosa, desinformació o malinformació. Tot i que les víctimes dels *deepfakes* no es limiten a les celebritats, l'espai del conjunt de fans és una frontera viable que pot creuar aquesta tecnologia per produir-hi danys econòmics⁴⁶.

4. Estudi jurídic de les vulneracions de drets d'imatge i veu de casos comentats

Els *deepfakes* representen una amenaça creixent per als drets d'imatge i veu de figures públiques, especialment esportistes, en explotar la seva identitat sense consentiment.

Casos com els de Lionel Messi i Gareth Southgate il·lustren com els *deepfakes* poden usar-se per a frauds comercials o difamació, afectant la reputació i el valor econòmic.

Encara que el cas d'Eddie Irvine no va involucrar l'us de *deepfakes*, sí que es va produir una manipulació d'imatges i estableix un precedent per la protecció de la imatge acotada als esportistes enfront d'usos comercials no autoritzats.

⁴⁵ GUMMER, ALEX. (4/09/2024) *Unlocking sponsorship success: new study reveals new ways of transforming sports sponsorships for maximum impact*. European Sponsorship Association Blog. <https://sponsorship.org/unlocking-sponsorship-success-new-study-reveals-new-ways-of-transforming-sports-sponsorships-for-maximum-impact/>

⁴⁶ PONDER, M.L., LEAK, T., MEGGS, K.E. (2023). *Deepfakes as Misinformation: The Next Frontier of Sports Fandom*. p 85. Capítol de: LANGMIA, K. (eds) *Black Communication in the Age of Disinformation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-27696-5_4

El cas de Mario Draghi, encara que no és dins de l'àmbit esportiu, sí és un cas europeu que fa paleses vulneracions similars aplicables a atletes, reforçant la necessitat de marcs legals robustos.

Normes com el GDPR, l'AI Act i lleis nacionals ofereixen eines legals, però l'aplicació és complexa a causa de l'anonimat digital i la jurisdicció transfronterera.

Els esportistes, figura concreta analitzada en aquest treball, poden exigir l'eliminació dels vídeos falsos, demandar per danys a la seva imatge o reputació, i presentar queixes davant autoritats de protecció de dades. No obstant això, trobar als responsables és difícil a causa de l'anonimat a internet.

4.1 Cas Eddie Irvine v. Talksport Ltd

És rellevant començar l'estudi dels casos amb el cas *Eddie Irvine v. Talksport Ltd* ja que encara que no va involucrar *deepfakes*, els principis legals emprats per resoldre aquest cas i les circumstàncies són aplicables a casos moderns de manipulació digital, com els *deepfakes* en l'àmbit esportiu protagonistes d'aquest estudi.

Aquest cas aborda l'ús no autoritzat de la imatge d'un esportista, establint un precedent rellevant per a la protecció de drets d'imatge al Regne Unit.

La sentència es va basar en el delictes de *passing off*, que protegeix contra la tergiversació que indueix a error al públic sobre un *endorsement* comercial. El nucli del cas va ser determinar si l'ús de la imatge manipulada constituïa *passing off*, un delictes de dret consuetudinari que protegeix contra la tergiversació que indueix a error al públic sobre la relació entre una persona i un producte o servei. Protegeix a algú d'una altra persona que faci creure falsament que els seus productes o serveis estan relacionats amb ells. En aquest cas, l'any 2002, l'emissora Talksport va usar una imatge manipulada del pilot de Fórmula 1 Eddie Irvine en un anunci, suggerint que ell recolzava la seva estació de ràdio. Irvine va demandar Talksport, i el tribunal va dictaminar a la seva decisió que això era una tergiversació il·legal que danyava la seva reputació comercial.

No obstant, cal remarcar que el concepte de *passing off* emprat en aquesta sentència és un concepte no directament lligat amb la violació del dret d'imatge vinculat a la personalitat del

pilot, sinó més a prop de la usurpació de marca, que d'acord amb el tractament que la jurisdicció civil del Regne Unit dona, aquestes circumstàncies són emprades sota el concepte d'il·lícit civil estretament relacionat amb el Dret de marques. La usurpació de marca implica que un comerciant tergiversi d'algun mode els seus productes o serveis com si fossin els d'un altre comerciant, o viceversa.

El Tribunal Superior va reconèixer inicialment l'existència de *passing off*, però va atorgar només 2.000 lliures en danys. Irvine va apel·lar, i Talksport va presentar una contestació. El Tribunal d'Apel·lació⁴⁷ va confirmar l'existència de *passing off* i va augmentar els danys a 25.000 lliures, considerant l'impacte econòmic en la capacitat d'Irvine per a atreure *endorsements* comercials. El tribunal va determinar que Irvine posseïa una reputació significativa (condició aplicable a tots els casos analitzats en aquest estudi), que la imatge manipulada suggeria falsament el seu suport a Talksport i que això podia danyar i reduir el valor dels seus futurs contractes de patrocin.

El Tribunal d'Apel·lació va ampliar als considerants 81 a 84 i 110 a 118 de la seva sentència l'abast del *passing off* per a incloure casos de *false endorsement*, un desenvolupament significatiu en la protecció dels drets d'imatge de celebritats com els esportistes d'elit.

Aquest cas mostra que els esportistes poden protegir la seva imatge si algú l'usa sense permís per a fins comercials.

La sentència d'Irvine ha estat un referent en casos posteriors sobre drets d'imatge. En el cas *Fenty v. Arcadia Groups Band (2015)*⁴⁸, la cantant Rihanna va guanyar una demanda per *passing off* contra Topshop per vendre samarretes amb la seva imatge sense permís, ja que l'ús suggeria el seu *endorsement*. El tribunal va aplicar els principis d'Irvine citant-los als considerants 30-31, 3, 38 i 46 de la sentència, i destacant que la tergiversació ha de ser creïble per a un segment significatiu del públic. Aquest cas reforça l'aplicabilitat d'Irvine a contextos moderns, inclosos els *deepfakes*, on la manipulació digital pot induir a error de manera més convincent.

⁴⁷ ENGLAND AND WALES COURT OF APPEAL (CIVIL DIVISION). (01/04/2003). *Irvine & Ors v Talksport Ltd*. Casemine <https://www.casemine.com/judgement/uk/5b46f1ec2c94e0775e7ee2e2#>

⁴⁸ COURT OF APPEAL (CIVIL DIVISION). (22/01/2015) *Fenty v. Arcadia Groups Band (2015)* Case No: A3/2013/2087 & A3/2013/2955. Judiciary. <https://www.judiciary.uk/wp-content/uploads/2015/01/fenty-others-v-arcadia-others1.pdf>

És especialment rellevant per aquest estudi aquesta sentència i la vinculació amb la d'Irvine per distingir clarament els diferents i a la vegada entrelligats contextos dels drets de marca i de propietat intel·lectual amb els drets de la personalitat que inclouen el dret d'imatge i veu analitzats en aquest treball. La sentència del cas de Rihanna citada és l'apel·lació feta a la divisió de propietat intel·lectual de l'Alt Tribunal de Justícia del Regne Unit i és analitzada també per l'Organització Mundial de la Propietat Intel·lectual (OMPI) inclosa en materia de marques, no de dret d'imatge tot i utilitzar Topshop la imatge d'aquesta per lucrar-se. Permet per tant distingir el tractament jurisprudencial en base als drets en els que s'emparen (de marca i propietat intel·lectual o d'imatge) les peticions de les parts.

Un altre precedent rellevant és *Douglas v. Hello! Ltd* (2001)⁴⁹, on Michael Douglas i Catherine Zeta-Jones van demandar a una revista per publicar fotos no autoritzades del seu casament que ja havien venut en exclusivitat a una altra revista. El cas es va desenvolupar al llarg de 3 judicis entre 2001 i 2005 que va finalitzar amb *Douglas & Ors v. Hello! Ltd & Ors* [2007] UKHL 21 (02 May 2007)⁵⁰. La sentència del cas es va centrar en la privacitat i el tribunal va reconèixer el valor comercial de la imatge de les celebritats assignant 1.033.156 de lliures esterlines a la revista OK! a la qual havien venut en exclusiva les imatges del casament, un principi que complementa l'enfocament d'Irvine sobre el mal econòmic. En el context de *deepfakes*, aquest cas suggereix que l'explotació no autoritzada de la imatge pot generar indemnitzacions significatives.

La sentència *Edgar Davids v. Riot Games* (2017)⁵¹ també és pertinent. El futbolista holandès Edgar Davids va demandar al desenvolupador de videojocs Riot Games per utilitzar la seva imatge en un personatge (*Lucian Striker*) del seu videojoc *League of Legends* sense consentiment, i el tribunal holandès va reconèixer una violació dels drets d'imatge, atorgant

⁴⁹ Teacher Law. (Novembre de 2013). *Douglas v Hello Ltd. (No.1)*
<https://www.lawteacher.net/cases/douglas-v-hello.php?vref=1>

⁵⁰ HOUSE OF LORDS. OPINIONS OF THE LORDS OF APPEAL FOR JUDGMENT IN THE CAUSE. (02/05/2007). *Douglas & Ors v. Hello! Ltd & Ors* [2007] UKHL 21 (02 May 2007) Bailii Databases.
<https://www.bailii.org/uk/cases/UKHL/2007/21.html>

⁵¹ RECHTBANK AMSTERDAM. (09/08/2017). *Edgar Davids v. Riot Games* (2017) C/13/614861 / HA ZA 16-914 <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2017:5415>

danys que haurien de ser evaluats. Al considerant 4.13 de la sentència es cita l'article 21 de la Llei de Drets d'Autor holandesa aclarint que pot fer referència tant a interessos personals (la privacitat) com comercials. Es cita igualment la protecció derivada de l'article 8 del CEDH, que no es limita a les activitats privades, sinó que s'aplica també a les activitats professionals o empresarials. La norma establerta en l'article 21 de la Llei de Dret d'Autor implica que els retratats (Edgar Davids en aquest cas) no tenen per què en tots els casos permetre que la popularitat que han adquirit en l'exercici de la seva professió sigui explotada comercialment publicant les seves imatges o representacions sense rebre una compensació per això.

Aquest cas il·lustra com els principis d'Irvine s'apliquen en entorns digitals com és el cas dels videojocs (*League of Legends*), rellevants per a *deepfakes* que recreen la imatge d'esportistes. Cal remarcar novament però, la distinció i a la vegada vincle entre dret de marca, propietat intel·lectual i drets de la privacitat i la personalitat (imatge i veu entre ells) doncs es poden produir vulneracions simultànies que afectin diversos drets a la vegada i caldrà per tant, aplicar distinció a l'hora de considerar unes circumstàncies subsumibles a una norma jurídica o altra.

4.2 Cas Lionel Messi i *deepfake Wildcat Dive*

El 2023, un *deepfake* difós a Instagram i YouTube va mostrar a Lionel Messi promocionant l'aplicació fraudulenta *Wildcat Dive* que donava peu a una estafa piramidal. Per fer-ho van utilitzar fragments manipulats d'una entrevista real. Aquest ús no autoritzat de la seva imatge i veu vulnera múltiples normes. El contingut va utilitzar gravacions públiques de Messi manipulades mitjançant IA, ometent qualsevol identificació com a material artificial. Des del punt de vista jurídic, aquest acte vulnera el Reglament (UE) 2016/679 (GDPR), i la prohibició del tractament de dades biomètriques (com la seva imatge i veu) sense consentiment explícit (art. 9.1), incorrent en una infracció dels principis de licitud i transparència (art. 5.1), sancionable amb multes de fins a 20 milions d'euros (art. 83.5. a). Així mateix, el Reglament (UE) 2024/1689 (AI Act) exigeix en el seu article 50.1 que el contingut generat per IA sigui identificat com a tal. La omisió en aquest cas l'alinea amb les pràctiques prohibides de l'article 5.1.b, que veta sistemes d'IA dissenyats per a causar danys mitjançant l'engany propi dels *deepfakes*. Sota el GDPR (art. 17), Messi podria exigir l'eliminació immediata del *deepfake* d'Instagram i YouTube. El Reglament de Serveis Digitals

(UE) 2022/2065⁵² reforça aquesta obligació, exigint a les plataformes actuar ràpidament contra contingut il·legal.

Val la pena citar el cas *Polish DPA v. Meta* (2024) en el qual l'Autoritat Polonesa de Protecció de Dades va ordenar a Meta cessar la difusió d'anuncis *deepfake* que utilitzaven imatges de figures públiques sense consentiment, aplicant l'article 66 del GDPR i l'article 70(1)(2) del *Polish Data Protection Act*⁵³. Aquest precedent suggereix que les plataformes on es viralitzen els *deepfakes* de Messi podrien enfrontar sancions administratives si no es fan responsables i eliminen aquest contingut fraudulent. Val la pena igualment citar la *Cassazione Civile, Sez. I, 2 maggio 1991, n. 4785* d'Itàlia⁵⁴. Aquesta sentència va establir que l'ús no autoritzat de la imatge per a fins comercials viola els drets de personalitat, un principi aplicable si el cas de Messi s'hagués de litigar en un context europeu.

A nivell nacional, degut amb l'especial vincle de Messi amb l'estat espanyol, es podria produir el litigi sota la norma espanyola. Aquest *deepfake* també infringeix la Llei orgànica 1/1982. L'article 7.5 tipifica com a intromissió il·legítima l'ús no autoritzat de la imatge o veu, permetent a Messi reclamar la cessació del contingut i una indemnització per danys com la tipificada a l'art. 9.3. A més, l'article 11 de la Llei 3/1991, de Competència Deslleial⁵⁵, sanciona els actes que aprofiten indegudament la reputació aliena, aplicable el citat article a l'ús fraudulent que va afectar la imatge comercial de Messi, vinculada a contractes amb patrocinadors i marques com Adidas. En aquest cas concret l'absència d'accions legals documentades pot deure's a la dificultat d'identificar als responsables, donada la naturalesa anònima de les plataformes digitals. No obstant això, l'evidència suggereix que aquest cas infringeix drets de personalitat, i Messi o els seus representants podrien haver sol·licitat la

⁵² UE. (2022). Reglament (UE) 2022/2065 del Parlament Europeu i del Consell, de 19 d'octubre de 2022, sobre un mercat únic de serveis digitals i per el que es modifica la Directiva 2000/31/CE (Llei de Serveis Digitals). DOUE, L 277, 1-102.
[https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32022R2065\[\]](https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32022R2065[])(<https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32022R2065>)

⁵³ UODO (2024) *Polish DPA v. Meta* (2024)UODO (Poland) - DS.523.4486.2024.
[https://gdprhub.eu/index.php?title=UODO_\(Poland\)_-_DS.523.4486.2024](https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DS.523.4486.2024)

⁵⁴ CORTE DI CASSAZIONE CIVILE (1992). *Cassazione I civile; sentenza 2 maggio 1991, n. 4785; Pres. Scanzano, Est. Vercellone, P.M. Amirante (concl. parz. diff.); Soc. Mac (Avv. Bassani) c. Armani e Soc. Armani (Avv. Marone, Ceresi, Cattaneo, Pinotti) e Comitato italiano fodere. Cassa App. Milano 5 settembre 1986. Il Foro Italiano*, 115, 831/832-841/842. p 831 <https://www.jstor.org/stable/23186621>

⁵⁵ *Llei Orgànica 3/1991, de 10 de gener, de competència deslleial* (1991). BOE, num. 10, pp. 664-666.
<https://www.boe.es/buscar/act.php?id=BOE-A-1991-628>

retirada del contingut o iniciat procediments civils per danys i perjudicis, encara que no s'ha informat públicament.

Tals manipulacions generen perjudicis econòmics i ètics al erosionar la confiança pública en l'esportista i el futbol com a institució, així com als clubs amb els quals el públic general vinculen la seva figura.

4.3 - Cas Southgate

En aquest cas sobre el seleccionador de l'equip de futbol d'Anglaterra i el muntatge amb *deepfake* on feia comentaris fora de lloc sobre els seus jugadors, la *Football Association* (FA), entitat responsable de la selecció nacional i del futbol professional a tota Anglaterra, va qualificar els vídeos de "ofensius" i va anunciar que prendria mesures per a la seva eliminació, indicant una resposta activa per protegir la reputació de Southgate⁵⁶. Encara que no es va documentar una acció judicial específica, aquest incident podria qualificar-se com una vulneració dels drets d'imatge sota la legislació britànica, incloent-hi la Llei de Difamació de 2013⁵⁷. La creació i difusió de contingut fals que danya la reputació d'una figura pública pot considerar-se difamatòria, i la FA podria haver sol·licitat la retirada del contingut mitjançant notificacions legals a les plataformes. Per figures públiques com Southgate, es requereix provar malícia real, la qual cosa és plausible donada la naturalesa intencionadament falsa dels *deepfakes*. A més, l'ús no autoritzat de la seva imatge i veu podria considerar-se una violació de drets d'imatge, seguint el precedent d'*Irvine v. Talksport Ltd.*

D'altra banda també entra en joc l'article 8 del CEDH, que protegeix la vida privada i el cas *Peck v. el Regne Unit* que reforça que la publicació d'informació privada sense consentiment és sancionable, un principi aplicable al cas de Southgate.

Tot i així, la falta de traçabilitat en les plataformes digitals complica la persecució legal, però la resposta de la FA suggereix una intenció d'abordar la vulneració. Experts com Hany Farid

⁵⁶ MILMO, DAN & HERN, ALEX. (14/07/2024) *Deepfake clips of Gareth Southgate swearing after England match go viral*. TheGuardian.
<https://www.theguardian.com/technology/article/2024/jul/14/deepfake-gareth-southgate-england-football-team-euro-2024>

⁵⁷ *Enterprise and Regulatory Reform Act 2013*. Legislation.gov.uk
<https://www.legislation.gov.uk/ukpga/2013/26/contents>

han destacat la necessitat d'equilibrar la regulació amb la sàtira, assenyalant que vídeos com aquests, que usen la veu i la imatge de Southgate de manera ofensiva, atravessen la línia cap al mal reputacional⁵⁸.

4.4 - Cas Mario Draghi

EL 2023, un *deepfake* de Mario Draghi el mostrava promocionant inversions fraudulentess, afectant fins a 45 persones. Encara que no és un esportista, el cas és rellevant per l'àmbit esportiu per la seva similitud amb el de Messi i pel fet de tractar-se d'una figura pública amb una major exposició i vulnerabilitat a patir aquesta mena de muntatge. El GDPR també és d'aplicació en aquest cas, donat el tractament no autoritzat de dades biomètriques.

La legislació italiana ofereix un major nivell de protecció, fins i tot en absència d'una nova legislació *ad hoc*. De fet, encara que ja estan sobre la taula algunes propostes de nova regulació de la IA a Itàlia, l'antic marc jurídic és perfectament capaç de fer front als riscos que presenten els *deepfakes*.

Segons la legislació italiana, els *deepfakes* es consideren reproduccions de continguts convincents d'imatge, àudio i vídeo que constitueixen tant una violació dels drets de la personalitat de l'individu les característiques i els trets del qual subjectius es repliquen, com una violació dels drets d'aquest individu a la seva pròpia imatge.

De fet, segons la jurisprudència italiana, el dret a la pròpia imatge forma part dels denominats drets inviolables de la personalitat consagrats en l'article 2 de la Constitució italiana, que inclouen aquells drets que es refereixen a aspectes essencials de la personalitat humana.

A més de la protecció constitucional dels drets de la personalitat, el dret a la pròpia imatge està regulat per l'article 10 del Codi Civil italià⁵⁹, que defineix l'abús del dret a la imatge com l'ús no autoritzat de la imatge d'una altra persona i preveu la indemnització per danys i perjudicis de qualsevol tercer que exposi o publiqui la imatge d'una persona “fora dels casos en què l'exposició o publicació estigui permesa per la llei” o “amb perjudici del decòrum o la

⁵⁸ Op cit 21

⁵⁹ REPUBBLICA ITALIANA. (1942) *Regio Decreto 16 marzo 1942, n. 262 Approvazione del testo del Codice civile*. Gazzetta Ufficiale della Repubblica Italiana. <https://www.gazzettaufficiale.it/dettaglio/codici/codiceCivile>

reputació de la pròpia persona” (aquesta disposició també pot ser invocada pels hereus de la persona retratada). En altres paraules: una imatge no pot exposar-se ni comercialitzar-se⁶⁰.

Per a un esportista en una situació similar, les mateixes normes serien aplicables, amb sancions civils i administratives per l'explotació il·lícita de la seva imatge. La jurisprudència a *Cassazione Civile, Sez. I, 2 maggio 1991, n. 4785*⁶¹ estableix que l'ús no autoritzat de la imatge per a fins comercials és una violació dels drets de personalitat, un principi aplicable a aquest cas.

5. Propostes de futur per a la protecció dels drets d'imatge i veu dels esportistes

5.1 - Propostes de regulacions futures i guies de bones pràctiques en l'àmbit esportiu

La proliferació de deepfakes planteja una amenaça significativa per als drets de la personalitat dels esportistes. L'explotació no autoritzada de la seva identitat digital no sols compromet la seva reputació, sinó també el seu valor econòmic, afectant contractes de patrocini i la confiança pública. Aquest apartat proposa un enfocament multifacètic que busca combinar reformes normatives, guies de bones pràctiques realistes degut a les complicacions que sempre genera crear una norma suficientment ferma com pot ser un Reglament a nivell comunitari europeu i, proposar idees de solucions tecnològiques basades en *blockchain* per salvaguardar els drets d'imatge i veu dels atletes, alineant-se amb principis ètics i legals.

Per contrarestar els riscos dels *deepfakes*, és imperatiu enfortir els marcs legals existents. Una proposta clau és l'adaptació del Reglament (UE) 2024/1689 (AI Act) al context esportiu, incorporant disposicions específiques que exigeixin el consentiment exprés per a l'ús de la imatge o veu dels esportistes en continguts generats per IA. Aquesta adaptació ha de tenir en compte tots els matisos i impacte no només econòmic i reputacional sinó permetre elaborar un protocol de valoració de danys que puguin afectar al rendiment esportiu de l'atleta. Cal informar també al esportistes i les organitzacions de l'existència de l'avaluació de l'interès legítim (LIA). Encara que no es descriu explícitament en el GDPR, l'avaluació de l'interès

⁶⁰ Op cit 8

⁶¹ Op cit 51

legítim és una forma d'avaluació de riscos que ha de realitzar-se quan el tractament de dades personals es basa en un interès legítim com pot ser un contracte de patrocini o de drets televisius que el propi esportista o el seu equip/federació firma. Cal tenir en compte que es recolliran dades de l'atleta i es publicitaran, i aquestes poden incloure les dades biomètriques que serveixin de base per manipulacions d'imatges a través de la tecnologia *deepfake*.

La LIA recolza la legalitat del tractament de dades i demostra que s'ha fet correctament el treball preliminar per determinar que l'interès legítim és una base legal adequada, confirma el seu compliment i li permet alinear-se amb el principi de responsabilitat.

L'article 50 de l'AI Act, que imposa obligacions de transparència per a sistemes d'IA de risc limitat, podria complementar-se amb requisits d'etiquetatge obligatori i verificació d'autenticitat en l'àmbit esportiu, prevenint així la difusió de *deepfakes* enganyosos. Aquesta reforma s'alinea amb els principis ètics de la UNESCO sobre la intel·ligència artificial, que advoquen per la transparència i el respecte als drets humans⁶².

Paral·lelament, les federacions esportives, com la FIFA o el COI, han de liderar la creació de guies de bones pràctiques. Aquestes guies podrien establir codis de conducta que obliguin a obtenir el consentiment informat dels atletes per a qualsevol contingut generat per IA, garantir la seva identificació com a artificial i proporcionar canals per reportar usos no autoritzats. Inspirades en els principis de la UNESCO, aquestes directrius fomentarien un ús ètic de la IA, protegint la dignitat dels esportistes i reforçant la confiança en l'ecosistema esportiu. Un estudi recent destaca l'eficàcia dels codis sectorials per a mitigar riscos tecnològics⁶³.

5.2 - Viabilitat jurídica del blockchain en la protecció dels drets de la personalitat i la protecció econòmica dels drets d'imatge i veu en l'era digital de la IA

La integració de la tecnologia *blockchain* ofereix una solució innovadora per protegir els drets d'imatge i veu dels esportistes enfront els *deepfakes* i la problemàtica del consentiment

⁶² Op cit 2

⁶³ Op cit 38

que pugui donar o no, d'una forma més còmoda i/o automatitzada, l'esportista en qüestió o el seu pertinent representant legal.

En aquest treball es planteja proposar la creació d'un sistema de llicències basat en *blockchain* que utilitzi contractes intel·ligents (*smart contracts*)⁶⁴ per regular l'ús lícit de la identitat digital dels atletes. En aquest model, els esportistes podrien registrar els seus drets d'imatge i veu en una plataforma *blockchain*, creant un registre immutable i transparent permetent als esportistes controlar qui utilitza les seves imatges o vídeos, evitant usos no autoritzats com els *deepfakes*. Per exemple, poden també crear col·leccionables digitals i rebre pagaments automàtics pel seu ús. Les entitats interessades, com fundacions d'equips, federacions esportives o acadèmies juvenils, sol·licitarien llicències mitjançant contractes intel·ligents, que executarien automàticament els termes acordats, incloent-hi la compensació i les limitacions d'ús. Aquest sistema garantiria el control de l'atleta sobre la seva identitat, evitant vulneracions com els *deepfakes* i complint amb l'article 50 del AI Act.

Entre les principals aplicacions de *blockchain* en l'esport es troben la venda segura d'entrades, els *tokens* per a aficionats, els col·leccionables digitals, la gestió de dades d'esportistes i els contractes intel·ligents per a patrocinis. Aquestes aplicacions ajuden a millorar la transparència, el compromís i l'eficiència operativa. Per citar dos exemples reals, al juny de 2020, el FC Barcelona va presentar la seva oferta de fitxes d'aficionat (FTO) a través de l'apartat socis de la seva pàgina web. Va aconseguir recaptar 1,3 milions de dòlars en dues hores. Els *tokens* d'aficionat ofereixen als seguidors l'oportunitat de participar en les decisions del club, gaudir de continguts i connectar estretament amb l'equip. Aquesta ràpida recaptació de fons demostra l'interès que desperten els actius entre els aficionats a l'esport. Un segon exemple és el de la UEFA, que va introduir una aplicació mòbil de venda d'entrades basada en *blockchain* per al torneig *Euro 2020*. Aquesta aplicació va millorar la seguretat i la transparència en la distribució d'entrades, al mateix temps que evitava el frau i facilitava la transferència d'entrades entre aficionats. L'ús de la tecnologia *blockchain* per part de la UEFA va millorar l'experiència de compra d'entrades per als aficionats⁶⁵.

⁶⁴ STUART D. LEVI AND ALEX B. LIPTON, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP. (26/05/2018). *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*. Harvard Law School Forum on Corporate Governance. <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>

⁶⁵ A3LOGICS. (19/11/2024). *Blockchain in sports: Use cases, advantages and challenges*. <https://www.a3logics.com/blog/blockchain-in-sports/>

Aquest exemple mostra com un dels clubs esportius més importants del món com és el FC Barcelona o una de les principals organitzacions a nivell europeu ja estan familiaritzats i han fet ús d'aquest tipus de tecnologia.

En el sector de l'esport, l'emmagatzematge segur de dades i la transparència són essencials. La naturalesa descentralitzada del *blockchain* garanteix una gestió de dades segura i a prova de manipulacions, la qual cosa és crucial per a dades sensibles com les seves imatges, les mètriques de rendiment dels atletes i els registres de salut⁶⁶.

La viabilitat jurídica d'aquest sistema es fonamenta en la seva compatibilitat amb el dret contractual i el GDPR. Els contractes intel·ligents, quan compleixen els requisits d'oferta, acceptació i contraprestació, són executables sota els marcs legals existents. Per complir amb el GDPR, la plataforma hauria d'incorporar mecanismes de protecció de dades, com l'emmagatzematge de *hashes* de consentiments en lloc de dades personals completes, assegurant la privacitat dels atletes. La literatura acadèmica avala l'eficàcia del *blockchain* per a la gestió de drets digitals, destacant una reducció significativa en usos no autoritzats com a través del sistema *DRMChain*⁶⁷.

Per contrarestar aquests riscos, els esportistes i les organitzacions esportives han d'adoptar estratègies proactives de gestió reputacional. Això inclou campanyes educatives per sensibilitzar al públic sobre els *deepfakes*, fomentant una major "alfabetització digital" entre els aficionats. A més, l'adopció de tecnologies com *blockchain* pot garantir la traçabilitat i autenticitat del contingut, permetent als atletes controlar l'ús de la seva imatge i veu. Per exemple, els *smart contracts* podrien regular els usos autoritzats en campanyes publicitàries, reduint el risc d'explotació il·lícita.

No obstant, no es tracta la tecnologia *blockchain* d'una solució perfecta ni molt menys; un problema derivat de la naturalesa del *blockchain* és l'incompliment de les lleis de protecció de dades. Aquesta incompatibilitat es deu a l'arquitectura de xarxa distribuïda *peer-to-peer*⁶⁸, que la situa en desacord amb el paradigma de processament de dades centralitzat de les lleis de

⁶⁶ Ibid 64

⁶⁷ ZHAOFENG MA, MING JIANG, HONGMIN GAO, ZHEN WANG. (2018). *Blockchain for digital rights management*. Future Generation Computer Systems, Vol 89, p 746-764
<https://doi.org/10.1016/j.future.2018.07.029>.

⁶⁸ REAL ACADEMIA ESPAÑOLA. (s.d.). *P2P*. Diccionario panhispánico del español jurídico.
<https://dpej.rae.es/lema/p2p>

protecció de dades. Aquest contrast pot dificultar l'adaptació de les actuals lleis de protecció de dades amb els elements centrals del *blockchain*: descentralització, transparència i immutabilitat. Això últim, per exemple, no encaixa amb el dret a l'oblit i limitació del tractament del GDPR (articles 17 a 19) també conegut com a dret de supressió. En aquest sentit el TJUE s'ha mostrat ferm en la protecció d'aquest dret a l'oblit i la vinculació d'aquest amb les dades que s'emmagatzemen a Internet tal com es desprèn dels Considerants 65 i 66 de la *Sentència del TJUE (Gran Sala) de 24 de setembre de 2019. GC i altres contra Commission nationale de l'informatique et des libertés (CNIL)*⁶⁹. En aquesta sentència quatre individus van sol·licitar a l'autoritat francesa de protecció de dades (CNIL) que ordenés a Google desindexar enllaços a pàgines web amb dades sensibles, incloent-hi un fotomuntatge satíric de GC que representava una relació il·lícita. El TJUE va aclarir les condicions per a la desindexació sota l'article 17 del GDPR (dret a l'oblit), exigint un equilibri entre els drets de privacitat i l'interès públic en la informació. La sentència va subratllar que les imatges, com a dades personals, requereixen consentiment o una base legal per al seu processament, i que els operadors de motors de cerca, que utilitzen IA, són responsables d'avaluar sol·licituds de desindexació. Aquest cas aborda directament els drets d'imatge en el context de motors de cerca, que empren IA, i és aplicable al paradigma que es genera amb els *deepfakes* que difonen d'esportistes en plataformes digitals.

A part dels aspectes tècnics comentats anteriorment, la falta de regulacions legals de *blockchain*, així com la volatilitat de les criptomonedes pot representar un risc per a l'estabilitat financera que impedeixi la plena adaptació del *blockchain* en la indústria de l'esport.⁷⁰

⁶⁹ TJUE. (2019). *Sentència del TJUE (Gran Sala) de 24 de setembre de 2019. GC i altres contra Commission nationale de l'informatique et des libertés (CNIL)* Eur-Lex.
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62017CJ0136>

⁷⁰ BERKANI, AS., MOUMEN, H., BENHARZALLAH, S. ET AL (22/03/2024). *Blockchain Use Cases in the Sports Industry: A Systematic Review*. Int J Netw Distrib Comput 12, 17–40 (2024). p 34 i 35.
<https://doi.org/10.1007/s44227-024-00022-3>

6. Conclusions

1 - La irrupció de la intel·ligència artificial generativa, especialment a través de tecnologies com els *deepfakes*, ha posat en evidència les mancances del marc jurídic europeu vigent. El gran impacte que està tenint a la nostra societat la revolució de les IA està accentuant de forma massa evident la situació fàctica que es produeix a l'hora de crear lleis: aquestes es creen com a resposta reactiva a les circumstàncies que condicionen la vida en societat i no pas de forma proactiva per prevenir. S'està generant un problema cada cop major de ritmes desacompassats. D'aquesta manera les noves tecnologies i especialment les que evolucionen de forma més ràpida deixen desfasades amb la mateixa velocitat les lleis i normes jurídiques que es van creant. És per això que cal adoptar normes que utilitzin valors més atemporals (i per això difícilment adaptables i flexibles a totes les circumstàncies) que les permetin adaptar-se a les noves tecnologies que van sorgint. Normatives com el Reglament General de Protecció de Dades (GDPR) i el Reglament d'Intel·ligència Artificial (AI Act) ofereixen un punt de partida per a protegir dades personals i regular l'ús de la IA, però la seva aplicació a l'àmbit esportiu resulta limitada.

2 - Els esportistes, a causa de la seva condició de figures públiques, enfronten riscos específics relacionats amb els seus drets d'imatge i veu que no estan plenament coberts per aquestes lleis generals. L'abundància de dades biomètriques accessibles en retransmissions, xarxes socials i bases de dades públiques incrementa la seva exposició a manipulacions digitals, com la creació de *deepfakes*. Aquesta situació genera una notable inseguretat jurídica, ja que les eines legals actuals no estan dissenyades per respondre a la rapidesa i complexitat d'aquestes tecnologies emergents. Per exemple, un *deepfake* que alteri la imatge d'un atleta podria difondre's massivament abans que s'activi qualsevol mecanisme de defensa legal. Així, es fa evident la necessitat de reformes legislatives que contemplin les particularitats del sector esportiu, adaptant les normatives a aquest context i garantint una protecció més efectiva enfront dels avanços tecnològics.

3 - Els *deepfakes* no només constitueixen un desafiament jurídic, sinó que també desencadenen dilemes ètics profunds, especialment al afectar la confiança del públic en l'autenticitat de les figures esportives. La hipervisibilitat dels atletes, potenciada per plataformes digitals i mitjans de comunicació, agreuja les conseqüències d'aquestes manipulacions. Un vídeo fals d'un esportista pot tenir un impacte devastador en la seva reputació, fins i tot si es demostra la seva falsedat, degut a aquest efecte persistent en la

percepció pública i al mal psicològic que això genera. Aquest risc es veu amplificat per la velocitat de difusió en xarxes socials, on els continguts virals escapen fàcilment al control de l'afectat. Des d'un enfocament ètic, es requereix un marc que transcendeixi la mera regulació legal i fomenti principis com la veracitat, el respecte a la dignitat i la protecció de la integritat personal. Organismes com la UNESCO, mitjançant la seva Recomanació sobre l'Ètica de la Intel·ligència Artificial, subratllen la importància d'un ús responsable de la IA, un estàndard que hauria d'orientar les polítiques en l'àmbit esportiu per a mitigar aquests efectes nocius.

4 - L'AI Act classifica els *deepfakes* com a sistemes de “risc limitat”, una categorització que no reflecteix adequadament el seu impacte en l'àmbit esportiu. Per als esportistes, el “capital d'imatge” representa un actiu econòmic essencial, és el que determina els seus ingressos, i la seva alteració mitjançant IA pot ocasionar pèrdues significatives, tant a nivell personal com per a les entitats associades, com a clubs o patrocinadors. Per exemple, un *deepfake* que suggereixi un comportament indegut podria no sols comprometre els ingressos per contractes publicitaris de l'atleta, sinó també danyar la imatge del seu equip o federació. La desconfiança generada per continguts falsificats pot reduir l'atractiu dels atletes de cara a patrocinadors, disminuir el valor de contractes comercials i obligar els esportistes a incórrer en despeses addicionals, com ara assegurances contra riscos digitals o campanyes d'autenticació. Aquest fenomen requereix un marc legal que contempli la responsabilitat de les plataformes digitals i fomenti estratègies preventives, com l'educació del públic i la implementació de tecnologies de verificació, per tal de preservar el valor econòmic de l'esport. Aquesta subestimació del risc fa palesa una falta d'adaptació de l'AI Act a les dinàmiques específiques de l'esport, on la imatge pública té un valor tangible i estratègic. Per corregir aquesta deficiència, seria necessari reconsiderar la classificació de risc dels *deepfakes* en contextos d'alta exposició mediàtica, incorporant mesures específiques que protegeixin les figures públiques (incloent-hi les esportives) i reconeguin les implicacions econòmiques i socials d'aquestes tecnologies.

5 - Cal també introduir un nou factor temporal dins l'equació esportistes-IA doncs la carrera professional d'un esportista es desenvolupa generalment durant la seva joventut, quan en millor estat físic es troba aquesta persona, un cop finalitzada la plenitud física el rendiment va baixant fins que l'esportista es retira i, sovint, segueix vinculat a l'esport des d'una posició diferent. No és la mateixa situació professional que la d'una feina on per exemple va millorant la posició i les condicions econòmiques del treballador en funció de la seva

antiguitat i la carrera professional és més dil·latada en el temps. Una afectació a la carrera esportiva d'un atleta a causa d'un mal ús de les IA pot afectar la seva vida professional d'una forma relativament molt més agreujada que la d'un treballador d'un altre sector precisament per aquest factor de brevetat en la seva carrera professional de la mateixa manera que pot provocar que un cop retirat, una mala fama a causa de *deepfakes* associada a la seva figura quan encara competia, encara que se n'hagi demostrat la falsedat, pot provocar que aquest esportista retirat no pugui seguir vinculat a l'esport d'una manera diferent. Per posar un exemple, una persona que com a jugador va patir *deepfakes* on se'l veia consumint i tot i ser fals, se l'associi amb les drogues i per tant no se'l consideri pel càrrec d'entrenador o similar un cop ja retirat.

6 - L'heterogeneïtat de les legislacions nacionals a la Unió Europea, combinada amb la naturalesa transnacional de les plataformes digitals, dificulta la protecció efectiva dels drets dels esportistes enfront dels *deepfakes*. Encara que l'AI Act pretén unificar criteris a nivell europeu, la difusió de continguts falsificats a través de plataformes globals planteja problemes jurisdiccionals complexos. Un *deepfake* creat fora de la UE però accessible a Europa podria evadir les sancions comunitàries, deixant als atletes en una posició vulnerable. Aquesta descoordinació exigeix una resposta supranacional que vagi més enllà de l'harmonització legislativa i inclogui acords internacionals amb plataformes digitals i organismes globals. Només mitjançant una col·laboració transfronterera es podrà establir un sistema de responsabilitat compartida que garanteixi l'aplicació efectiva de les normes i la protecció dels drets en un entorn digital sense fronteres.

7 - La sofisticació de les xarxes generatives adversatives i l'absència d'eines de detecció en temps real representen obstacles tècnics significatius per a prevenir l'ús indegut de la imatge i veu dels esportistes. La viralització instantània de *deepfakes* en plataformes digitals agreuja aquest problema, ja que el mal reputacional pot consolidar-se abans que el contingut sigui identificat i retirat. Això posa en relleu la necessitat d'imposar obligacions més estrictes a les plataformes, com el desenvolupament de sistemes automatitzats de detecció i la col·laboració amb federacions esportives per a establir bases de dades de contingut autèntic. Sense avanços tecnològics que permetin una resposta proactiva, els esportistes continuaran depenent de mesures reactives que arriben tard per mitigar els efectes d'aquestes manipulacions.

8 - La jurisprudència existent citada, com els casos *Eddie Irvine v. Talksport Ltd* o *Fenty v. Arcàdia Group*, proporciona principis útils per a abordar l'ús no autoritzat de la imatge, però

la seva aplicació als *deepfakes* des de la perspectiva del dret de la personalitat en l'esport és limitada. La falta de precedents específics sobre manipulacions digitals a través de *deepfakes* en el món de l'esport que hagin dut a casos on la qüestió jurídica analitzada sigui el dret de la personalitat concretant-se en imatge i/o veu redueix la predictibilitat judicial i subratlla la necessitat d'una regulació adaptada. Els tribunals europeus haurien de liderar el desenvolupament d'una jurisprudència específica, establint bases que orientin futurs litigis en aquest àmbit emergent i concret dels drets de la personalitat d'imatge i veu acotats a la figura dels esportistes.

9 - L'ús de *blockchain* i *smart contracts* per gestionar hipotètiques llicències d'imatge ofereix una solució innovadora al permetre un control transparent de la identitat digital. No obstant això, la seva implementació enfronta reptes legals, com la incompatibilitat amb el dret a l'oblit del GDPR, i tècnics, com la necessitat d'estàndards universals. Superar aquestes barreres requereix un esforç conjunt entre legisladors i tecnòlegs per a garantir la seva viabilitat en el context esportiu.

10 - Federacions com la FIFA, UEFA, el COI o similars podrien promoure guies ètiques per l'ús de la IA, però el seu impacte és limitat sense mesures vinculants a nivell legal. Aliances amb legisladors de les nacions que aquestes federacions acullen i amb plataformes digitals són essencials per a establir estàndards globals o, si més no europeus, que reforcin la protecció dels esportistes enfront dels *deepfakes*.

11 - D'altra banda, seria també positiu el dur a terme una alfabetització digital per conscienciar al públic sobre els *deepfakes*, però ha d'integrar-se en un enfocament més ampli que combini legislació, tecnologia i ètica. Campanyes dirigides a aficionats i patrocinadors són útils perquè aquests puguin reconèixer o si més no ser conscients del risc existent amb el contingut que es publica a les xarxes socials i plataformes, però no substitueixen la necessitat de sancions legals efectives.

12 - En conclusió, protegir els drets d'imatge i veu a l'àmbit de l'esport requereix una estratègia coordinada que abordi els aspectes normatius, tecnològics i ètics. La inacció podria danyar la integritat dels atletes i la confiança en l'esport, fent imprescindible una col·laboració entre tots els actors involucrats.

7. Bibliografia

Documents

- Jurisprudència

CORTE DI CASSAZIONE CIVILE (1992). *Cassazione I civile; sentenza 2 maggio 1991, n. 4785; Pres. Scanzano, Est. Vercellone, P.M. Amirante (concl. parz. diff.); Soc. Mac (Avv. Bassani) c. Armani e Soc. Armani (Avv. Marone, Ceresi, Cattaneo, Pinotti) e Comitato italiano fodere. Cassa App. Milano 5 settembre 1986. Il Foro Italiano*, 115, 831/832-841/842. p 831 <https://www.jstor.org/stable/23186621>

COURT OF APPEAL (CIVIL DIVISION). (22/01/2015) *Fenty v. Arcadia Groups Band (2015) Case No: A3/2013/2087 & A3/2013/2955*. Judiciary. <https://www.judiciary.uk/wp-content/uploads/2015/01/fenty-others-v-arcadia-others1.pdf>

ENGLAND AND WALES COURT OF APPEAL (CIVIL DIVISION). (01/04/2003). *Irvine & Ors v Talksport Ltd*. Casemine <https://www.casemine.com/judgement/uk/5b46f1ec2c94e0775e7ee2e2#>

ENGLAND AND WALES HIGH COURT (CHANCERY DIVISION) DECISIONS. (13/03/2002). *Edmund Irvine Tidswell Ltd. v Talksport Ltd. [2002] EWHC 367 (Ch) (13th March, 2002)*. BAILII Databases. <https://www.bailii.org/ew/cases/EWHC/Ch/2002/367.html>

HOUSE OF LORDS. OPINIONS OF THE LORDS OF APPEAL FOR JUDGMENT IN THE CAUSE. (02/05/2007). *Douglas & Ors v. Hello! Ltd & Ors [2007] UKHL 21 (02 May 2007)* Bailii Databases. <https://www.bailii.org/uk/cases/UKHL/2007/21.html>

RECHTBANK AMSTERDAM. (09/08/2017). *Edgar Davids v. Riot Games (2017) C/13/614861 / HA ZA 16-914* <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2017:5415>

Teacher Law. (Novembre de 2013). *Douglas v Hello Ltd. (No.1)*. <https://www.lawteacher.net/cases/douglas-v-hello.php?vref=1>

TEDH. (28/01/2003) *Peck v. the United Kingdom*, Application No. 44647/98 (2003). <https://hudoc.echr.coe.int/eng?i=001-60898>

TEDH. (15/04/2009). *Case of Reklos and Davourlis v. Greece* (application no. 1234/05) HUDOC . <https://hudoc.echr.coe.int/eng?i=001-90617>

TEDH. (07/02/2012). *STS Asunto Von Hannover c. Alemania (no 2)*, Demandas nos 40660/08 et 60641/08). <https://hudoc.echr.coe.int/eng?i=001-139414>

TEDH. (2023). *Cas Glukhin v. Russia* (application no. 11519/20). Hudoc.
<https://hudoc.echr.coe.int/eng?i=001-225655>

TJUE. (2019). *Sentència del TJUE (Sala Segona) de 29 de juliol de 2019, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, C-40/17 29. Curia.
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=ES>

TJUE. (2019). *Sentència del TJUE (Gran Sala) de 24 de setembre de 2019, GC i altres contra Commission nationale de l'informatique et des libertés (CNIL)*. Eur-Lex.
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62017CJ0136>

UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA—WESTERN DIVISION. (04/03/2023). *Young v. NeoCortex, Inc.*, No. 2:23-cv-02496 (C.D. Cal. 2023).
<https://www.classaction.org/media/young-v-neocortex-inc.pdf>

UODO (2024) *Polish DPA v. Meta* (2024)UODO (Poland) - DS.523.4486.2024.
[https://gdprhub.eu/index.php?title=UODO_\(Poland\)_-_DS.523.4486.2024](https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DS.523.4486.2024)

- Documents d'organitzacions internacionals

i. UE

UE. (2016). *Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i per el que es deroga la Directiva 95/46/CE*. EUR-Lex.
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>

UE. (2022). *Reglament (UE) 2022/2065 del Parlament Europeu i del Consell, de 19 d'octubre de 2022, sobre un mercat únic de serveis digitals i per el que es modifica la Directiva 2000/31/CE (Llei de Serveis Digitals)*. DOUE, L 277, 1-102.
[https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32022R2065\[\]](https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32022R2065[])
<https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32022R2065>

UE. (2024). *Reglament (UE) 2024/1689 del Parlament Europeu i del Consell de 13 de juny de 2024 per el que s'estableixen normes armonitzades en matèria d'intel·ligència artificial i per el que es modifiquen els Reglaments (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 i les Directives 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Reglament d'Intel·ligència Artificial)*. DOUE, L 1689, 12.7.2024.
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689>

ii. Documents d'altres organitzacions internacionals

UNESCO. (25/06/2021) *Recomanació sobre l'ètica de la intel·ligència artificial*. pp. 5 i 6 <https://unesdoc.unesco.org/ark:/48223/pf0000377897>

- **Altres documents**

Enterprise and Regulatory Reform Act 2013. Legislation.gov.uk
<https://www.legislation.gov.uk/ukpga/2013/26/contents>

Gobierno de España, Secretaría de Estado de Digitalización e Inteligencia Artificial y Telecomunicaciones. (Març 2025.). *Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial*. Ministerio para la transformación digital y de la función pública.
https://avance.digital.gob.es/_layouts/15/HttpHandlerParticipacionPublicaAnexos.ashx?k=19128

Gobierno de España. (2023). Reial Decret 729/2023, de 27 d'agost, per el qual s'aprova l'Estatut de l'Agencia Espanyola de Supervisió d'Intel·ligència Artificial. BOE, núm. 210, 2 de setembre de 2023, pp. 122289-122316.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-18911

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. (1982). BOE, num. 115, pp. 12546-12548.
<https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196>

Llei Orgànica 3/1991, de 10 de gener, de competència deslleial (1991). BOE, num. 10, pp. 664-666. <https://www.boe.es/buscar/act.php?id=BOE-A-1991-628>

REPUBBLICA ITALIANA. (1942) *Regio Decreto 16 marzo 1942, n. 262 Approvazione del testo del Codice civile*. Gazzetta Ufficiale della Repubblica Italiana.
<https://www.gazzettaufficiale.it/dettaglio/codici/codiceCivile>

Doctrina i fonts

A3LOGICS. (19/11/2024). *Blockchain in sports: Use cases, advantages and challenges*.
<https://www.a3logics.com/blog/blockchain-in-sports/>

AEPD. (20/11/2020). *Blockchain (II): Conceptos básicos desde la protección de datos*.
<https://www.aepd.es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos>

ALONSO, C. (18/11/2024). *Deepfake: ¿qué es y cómo detectarlo?*. UNIR Revista.
<https://www.unir.net/revista/derecho/deepfake-que-es/>

ANSÓN PEIRONCELY, RAFAEL. (12/11/2024) *La regulación de los Deep Fakes. ¿Se pueden poner puertas al campo?* Blog Bufete Mas y Calvet
<https://mascalvet.com/la-regulacion-de-los-deep-fakes-se-pueden-poner-puertas-al-campo/>

BASS, DANIELLE F. & PENNING, NATHANIEL. (25/07/2023). *The Legal Issues Surrounding Deepfakes*. Honigman.
<https://www.honigman.com/the-matrix/the-legal-issues-surrounding-deepfakes>

BERKANI, AS., MOUMEN, H., BENHARZALLAH, S. ET AL (22/03/2024). *Blockchain Use Cases in the Sports Industry: A Systematic Review*. Int J Netw Distrib Comput 12, 17–40 (2024). p 34 i 35. <https://doi.org/10.1007/s44227-024-00022-3>

BOWYER, WILLIAM. (12/05/2021) *Deepfakes in the world of entertainment and sport – A danger or a new opportunity?* Mackrell.Solicitors Blog. p 1-2.
<https://www.lexology.com/library/document.aspx?g=108a8fb5-7693-4cfc-8acb-5eb645d63a7e>

BUSCA, NICK. (02/02/2021). *As biometrics boom, who owns athletes' data? It depends on the sport*. The Washington Post
<https://www.washingtonpost.com/sports/2021/02/02/athletes-biometrics-data-privacy/>

DIARI ARGENTÍ ÀMBITO. (23/10/2024). *Lionel Messi sufrió una "deepfake": utilizaron una entrevista suya para promocionar una estafa piramidal*
<https://www.ambito.com/deportes/lionel-messi-sufrio-una-deepfake-utilizaron-una-entrevista-suya-promocionar-una-estafa-piramidal-n6073788>

EVANS, BEN.(13/10/2023). *What is passing off? Legal advice, defences and remedies*. Harper James. <https://harperjames.co.uk/article/passing-off/>

GITAN CHOPRA, GITAN & JOHAR, MANNAT KAUR. (18/06/2024). *The Economic Ripple Effect of Deepfake Disruption*. International Finance Student Association.
<https://ifsa-network.com/publications/the-economic-ripple-effect-of-deepfake-disruption/>

GUMMER, ALEX. (4/09/2024) *Unlocking sponsorship success: new study reveals new ways of transforming sports sponsorships for maximum impact*. European Sponsorship Association Blog.
<https://sponsorship.org/unlocking-sponsorship-success-new-study-reveals-new-ways-of-transforming-sports-sponsorships-for-maximum-impact/>

HANCOCK, J. T., & BAIENSON, J. N. (2021). *The social impact of deepfakes*. Virtual Human Interaction Lab, Stanford University.. pp. 150-151
<https://vhil.stanford.edu/publications/social-interaction/social-impact-deepfakes>

JACOBACCI AVVOCATI en col·laboració amb JACOBACCI & PARTNERS. (23/09/2024). *AI and Deepfakes: EU and Italian Regulations*. Legal500.
<https://www.jacobacci-law.com/news-and-publications/ai-and-deepfakes-eu-and-italian-regulations>

JACOBACCI, EUGENIO. (20/09/2024). *AI and Deepfakes: EU and Italian Regulations*. Legal500. <https://www.jacobacci.com/en/publications/ai-and-deepfakes>

KARRAS, TERO & LAINE, SAMULI & AILA, TIMO. (29/03/2019). *AStyle-Based Generator Architecture for Generative Adversarial Networks*. arXiv:1812.04948v3 [cs.NE] Cornell University, p 1-2 <https://arxiv.org/pdf/1812.04948>

L. FENG, W. ZHOU, W. LIU, Y. -S. ONG i K. C. TAN. (Maig 2022). *Solving Dynamic Multiobjective Problem via Autoencoding Evolutionary Search*. IEEE Transactions on Cybernetics, vol. 52, no. 5, pp. 2649-2662, <https://ieeexplore.ieee.org/document/9210737>

LÓPEZ, MARTINA. (25/03/2024) *Alerta por deepfake de Lionel Messi para promover una aplicación fraudulenta* Newsletter welivesecurity. Noticias, opiniones y análisis de la comunidad de seguridad de ESET

<https://www.welivesecurity.com/es/estafas-enganos/alerta-deepfake-messi-utilizado-promover-aplicacion-fraudulenta/>

MARLYNN WEI M.D., J.D. (Actualitzat a 13/02/2024 i consultat 30/03/2025). *The Psychological Effects of AI Clones and Deepfakes. Concerns range from misuse to the potential impact on reputation and identity.* Psychology Today

<https://www.psychologytoday.com/us/blog/urban-survival/202401/the-psychological-effects-of-ai-clones-and-deepfakes>

MILMO, DAN & HERN, ALEX. (14/07/2024) *Deepfake clips of Gareth Southgate swearing after England match go viral.* TheGuardian.

<https://www.theguardian.com/technology/article/2024/jul/14/deepfake-gareth-southgate-england-football-team-euro-2024>

PARK, JENNIFER. (17/02/2024). *Biometric Data Collection in Professional Sports Reveals Holes in Privacy Law.* The Columbia Journal of Law & the Arts.

<https://journals.library.columbia.edu/index.php/lawandarts/announcement/view/685>

PÉREZ-CABRERO, ISABEL. (09/02/2021). *Los 'deepfakes' y su relación con los derechos de imagen: ¿cuál es el límite?* Blog Propiedad Intelectual e Industrial Garrigues

<https://blogip.garrigues.com/propiedad-intelectual/los-deepfakes-y-su-relacion-con-los-derechos-de-imagen-cual-es-el-limite>

REAL ACADEMIA ESPAÑOLA. (s.d.). *P2P*. Diccionario panhispánico del español jurídico.

<https://dpej.rae.es/lema/p2p>

ROMERO MORENO, FELIPE. (29/03/2024). *Generative AI and deepfakes: a human rights approach to tackling harmful content.* International Review of Law, Computers & Technology, 38(3)297-326.

<https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2324540#d1e481>

RÖSSLER, ANDREAS & COZZOLINO, DAVIDE & VERDOLIVA, LUISA & RIESS, CHRISTIAN & THIES, JUSTUS & NIESSNER, MATTHIAS (26/08/2019)

FaceForensics++: Learning to Detect Manipulated Facial Images. The Computer Vision Foundation, p 8

https://openaccess.thecvf.com/content_ICCV_2019/papers/Rossler_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images_ICCV_2019_paper.pdf

RUIZ DE VALBUENA, IRENE. (19/09/2023. ACTUALIZADO:20/09/2023 - 10:24 CEST). *Caso Almendralejo: La difusión de las imágenes manipuladas de menores desnudas es también una infracción de protección de datos.* El País Madrid - 19/09/2023 - 14:42

https://elpais.com/economia/2023/09/19/mis_derechos/1695125490_270661.html

SCOTT, LAURA. (30/06/2024). *'Deepfake' Southgate videos viewed by millions.* BBC Sport.

<https://www.bbc.com/sport/football/articles/cqqlvd3qy1lo>

SOURAV, SUBHAM. (11/05/2024). *Social Media and Athlete Privacy: Navigating Legal Boundaries*. Global Sports Policy Review.

<https://www.g-spr.com/post/social-media-and-athlete-privacy-navigating-legal-boundaries>

STUART D. LEVI AND ALEX B. LIPTON, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP. (26/05/2018). *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*. Harvard Law School Forum on Corporate Governance.

<https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>

TENA, PABLO & SALA, MIREIA. (26/03/2025). *Anteproyecto de Ley para el buen uso y gobernanza de la IA*. Blog de Propiedad Intelectual y Tecnologías Cuatrecasas.

<https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/anteproyecto-ley-buen-uso-gobernanza-ia>

VACCARI, C., & CHADWICK, A. (2020). *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*. Social Media + Society, 6(1). <https://doi.org/10.1177/2056305120903408>

ZHAOFENG MA, MING JIANG, HONGMIN GAO, ZHEN WANG. (2018). *Blockchain for digital rights management*. Future Generation Computer Systems, Vol 89.p 746-764

<https://doi.org/10.1016/j.future.2018.07.029>.