Vol. 37, nº 1

Réalités truquées et visages volés : l'UE risque-t-elle d'y perdre la face ?

La nécessité d'harmoniser les droits de la personnalité dans l'UE en réponse au développement de l'hypertrucage

Marie-Anne Du Sablon*

* Université de Montréal.]

[Note : cet article a été soumis à une évaluation à double anonymat.]

RÉSUMÉ

Cet article traite des défis juridiques posés par l'hypertrucage (*deepfake*) dans l'Union européenne (UE). Ces technologies mobilisant l'intelligence artificielle permettent de manipuler l'image et la voix d'individus, souvent sans leur consentement. Ceci peut causer de graves préjudices, notamment dans le cas des hypertrucages à caractère pornographique. D'autant plus que la législation européenne actuelle, notamment le *Règlement général sur la protection des données* (RGPD) et la *Loi sur l'intelligence artificielle*, ne protège pas adéquatement les victimes d'hypertucage. Au plan national, les recours varient d'un État membre à l'autre en fonction de leurs traditions juridiques respectives : le droit civil offre une meilleure protection des droits de la personnalité, contrairement à la common law, qui demeure plus restrictive. Cet article plaide ainsi en faveur d'une harmonisation des droits de la personnalité au sein de l'UE, en s'appuyant notamment sur le RGPD, pour offrir des recours efficaces et uniformes.

MOTS-CLÉS

Hypertrucage – Intelligence artificielle – Droits de la personnalité – Droit de l'Union européenne – Règlement général sur la protection des données.

ABSTRACT

This article addresses the legal challenges posed by deepfake technologies in the European Union (EU). These technologies, which use artificial intelligence, allow for the manipulation of individuals' images and voices, often without their consent. This can cause serious harm, particularly in cases of pornographic deepfakes, especially since the current European legislation – specifically the *General Data Protection Regulation* (GDPR) and the *Artificial Intelligence Act* – does not adequately protect victims of *deefaked* content. At the national level, legal remedies vary from one Member State to another, depending on their respective legal traditions: civil law generally offers stronger protection of personality rights, whereas common law remains more restrictive towards them. This article therefore advocates for the harmonization of personality rights within the EU, relying in particular on the GDPR, to provide effective and uniform remedies.

KEYWORDS

Deepfake – Artificial Intelligence – Personality Rights – European Union Law – General Data Protection Regulation.

I. INTRODUCTION

Dans les dernières années, la numérisation à grande échelle et l'innovation technologique rapide nous ont fait entrer dans un monde proche de la science-fiction où l'intelligence artificielle, même si elle n'a pas encore pris la forme d'un robot comme l'auraient prédit les meilleurs romans dystopiques, fait partie de notre vie quotidienne. Ses avantages s'accompagnent également de défis, comme discerner le vrai du faux dans un monde que certains qualifient de *post-vérité*. Cela est dû en grande partie aux « deepfakes » ou hypertrucages, ceux-ci qui permettent de manipuler la voix ou l'apparence d'une personne à l'aide d'outils d'intelligence artificielle. Par exemple, il est possible de recréer un acteur décédé pour qu'il joue dans la *grande finale* d'une énième franchise qu'Hollywood refuse de laisser derrière. Malheureusement, la plupart du temps, la personne victime de l'hypertrucage n'a pas consenti à l'utilisation de son identité. Des études ont d'ailleurs montré que cette technologie peut avoir de graves conséquences pour les personnes touchées, du traumatisme psychologique à l'atteinte irrémédiable à la réputation[1]. Les organes législatifs, en particulier l'Union européenne (ci-après « UE »), devraient donc réagir en conséquence pour protéger les victimes d'hypertrucages en assurant une protection plus ample de l'identité au moyen de l'intégration des droits de la personnalité. En conséquence, cet article examinera d'abord le contexte juridique actuel en Europe concernant les hypertrucages, pour ensuite aborder la nécessité d'une harmonisation au sein de l'UE et les véhicules législatifs potentiels pour y parvenir. En effet, une modification du *Règlement général sur la protection des données* (ci-après « RGPD ») semble être la voie la plus prometteuse vers une protection améliorée et unifiée, car elle pourrait faire office de fondement législatif à d'éventuelles normes visant plus précisément l'Intelligence artificielle (ci-après « IA ») et les hypertrucages.

1. Karolina MANIA, « Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study », (2024) 25(1) *Trauma, Violence & Abuse* 117, en ligne : <https://journals.sagepub.com> (consulté le 11 octobre 2024).

II. CONTEXTE JURIDIQUE

1. L'Union européenne

Tout d'abord, le concept a récemment été introduit pour la première fois dans la législation de l'UE à l'article 3(60) de la *Loi sur l'intelligence artificielle* (ci-après « loi sur l'IA »)[2]. Dans sa forme la plus courante, une vidéo « deepfake » utilise l'IA pour manipuler le visage ou la voix d'une personne et les juxtaposer sur le corps d'une autre personne afin de créer des images/vidéos réalistes d'événements n'ayant jamais eu lieu[3]. Cette technologie est rendue possible grâce au *deep learning* de l'IA[4], qui s'appuie sur un traitement de données souvent non supervisé[5]. Pour créer ce type de contenu, la technologie utilise ainsi des données biométriques[6] sur une personne afin de créer une représentation physique ou vocale quasi parfaite de la personne choisie. Par conséquent, toute création d'hypertrucage utilise une grande quantité de données biométriques pour atteindre ce niveau de réalisme. D'une part, cette technologie présente un grand potentiel pour une variété d'utilisations bénignes, comme l'amélioration des méthodes d'enseignement et l'obtention d'un réalisme sans précédent dans les films et les jeux vidéo. D'autre part, le fait est que, jusqu'à présent, les hypertrucages ont surtout été de nature pornographique, ciblant presque exclusivement les femmes[7]. De plus, il est important de soulever, surtout dans le cas des hypertrucages pornographiques, qu'il y a généralement deux victimes plutôt qu'une. Évidemment,

2. « Deepfake : contenu image, audio ou vidéo généré ou manipulé par l'IA qui ressemble à des personnes, des objets, des lieux, des entités ou des événements existants et qui semblerait faussement authentique ou véridique aux yeux d'une personne » ; Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 fixant des règles harmonisées en matière d'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (loi sur l'intelligence artificielle), art. 3(60) (ci-après « Loi sur l'IA »).
3. Regina RINI et Leah COHEN, « Deepfakes, Deep Harms », (2022) 22(2) *Journal of Ethics and Social Philosophy* 143, en ligne : <https://doi.org/io.z65s6/jesp.vzziz.16z8> (consulté le 13 octobre 2024).
4. Alexandra Rose BRIEGER, « Empowerment or exploitation: A qualitative analysis of online feminist communities' discussions of deepfake pornography », Masters, Uppsala Universitet, 2024.
5. Kalpana TYAGI, « Deepfakes, Copyright & Personality Rights: An Interdisciplinary Perspective », Conference Paper, 2022, en ligne : <https://www.researchgate.net/publication/359711219> (consulté le 11 octobre 2024).
6. Loi sur l'IA, préc., note 2, art. 34, 35.
7. SECURITY HERO, « 2023 State of Deepfakes: Realities, Threats, and Impact », (Security Hero, 2023), en ligne : <https://www.securityhero.io/state-of-deepfakes> (consulté 14 octobre 2024).

nous vient immédiatement à l'esprit la personne dont le visage est placé sur un corps qui n'est pas le sien, mais qu'en est-il du corps sans visage ? Si la personne a, espérons-le, consenti à l'activité sexuelle et à sa captation, elle n'a fort probablement pas consenti à ce que le visage de quelqu'un d'autre soit placé sur le sien. Cela illustre la question sous-jacente des données obtenues et traitées par les technologies d'hypertrucage, car elles le sont sans égard au consentement de la personne visée.

En réponse à la vague de numérisation des informations, qui entraîne par le fait même la multiplication des échanges de données personnelles par des moyens technologiques, l'UE a adopté le RGPD afin de réglementer le marché numérique et de protéger les personnes physiques par rapport à leurs données personnelles[8], conformément aux droits codifiés par les articles 8(1) de la *Charte des droits fondamentaux de l'Union européenne* (ci-après la « Charte »)[9] et 16(1-2) du Traité sur le fonctionnement de l'Union européenne (ci-après « TFUE »)[10]. Bien que le RGPD vise à « harmoniser la protection des libertés et droits fondamentaux des personnes physiques »[11] et à renforcer « la sécurité juridique et pratique pour les personnes physiques »[12], il n'aborde pas explicitement le phénomène de l'hypertrucage, étant donné que l'utilisation généralisée de cette technologie n'était pas encore un sujet de préoccupation en 2016. En fait, hormis l'article 50(4) de la loi sur l'IA, qui crée une obligation de transparence pour les contenus « deepfake »[13], aucun autre règlement de l'UE ne cible explicitement la question[14]. Il en résulte un vide juridique alarmant pour les victimes de contenu hypertruqué, pour lesquelles il importe moins d'être averties que « X contenu est réalisé à l'aide de logiciels d'hypertrucage » que de savoir comment elles peuvent exercer leur droit à l'oubli[15] ou être indemnisées pour le préjudice subi. Il apparaît donc clairement que le droit de l'UE ne protège pas

8. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), [2016] JO L 119/1, préambule 1 (ci-après « RGPD »).
9. *Charte des droits fondamentaux de l'Union européenne*, [2012] JO C326/391, art. 8(1) (ci-après « Charte »).
10. Traité sur le fonctionnement de l'Union européenne, [2012] JO C326/47, art. 16 (ci-après « TFUE »).
11. RGPD, préc., note 8, préambule 3.
12. *Id.*, préambule 7.
13. Loi sur l'IA, préc., note 2.
14. K. MANIA, préc., note 1.
15. RGPD, préc., note 8, art. 17.

suffisamment les individus pour leur permettre d'exercer pleinement leur droit au respect de la vie privée et à la protection des données[16] en ce qui concerne le développement des technologies d'hypertrucage.

2. Les États membres

Deuxièmement, en raison de l'absence de législation européenne introduisant des recours spécifiques aux « deepfakes », chaque État membre a son propre traitement de la question. Bien qu'il existe des différences, les juridictions de droit civil explorent l'idée générale des droits de la personnalité d'une manière similaire[17], tandis que les juridictions de common law traitent généralement cette question comme un délit civil, plus précisément comme un abus de confiance (*breach of confidence*) ou une usurpation d'identité (*passing off*). Il convient toutefois de noter que l'approche civile est à privilégier, entre autres, car elle est mieux adaptée au régime actuel du droit d'auteur. En effet, un système de protection proche du système actuel pour les droits d'auteur serait favorable en termes de cohérence et de simplicité. Il est logique que, si le droit d'auteur reconnaît les droits moraux d'un auteur, même dans les États de common law, cette logique doive également s'appliquer à la représentation d'une personne dans le cas des « deepfakes », indépendamment du choix d'une personne de commercialiser ou non son identité. En outre, l'UE est principalement composée d'États de droit civil, ce qui signifie qu'une grande partie de l'UE fonctionne déjà avec une conception des droits de la personnalité qui reconnaît à la fois les composantes commerciales et morales de l'image d'une personne facilitant grandement l'introduction d'un tel concept au niveau de l'UE.

2.1 États de droit civil

Dans les juridictions civilistes, il est reconnu que l'autonomie de la protection de l'image d'une personne est une composante de la protection de sa personnalité au sens large. Le principe du droit à l'image englobe donc à la fois le droit à la vie privée et les droits de la personnalité. En d'autres termes, une personne a des droits exclusifs sur sa propre représentation, pour autant que celle-ci soit *évidente*. Il ne suffit donc pas que la personne se reconnaisse dans une image,

16. Charte, préc., note 9, art. 7 et 8.
17. T. SYNODINOU, « Image Right and Copyright Law in Europe: Divergences and Convergences », (2014) 3 *Laws* 181, en ligne : <https://www.mdpi.com/journal/laws> (consulté le 12 octobre 2024).

il faut aussi que d'autres personnes la reconnaissent[18], ce qui peut imposer de sérieuses restrictions à la personne dont le corps est utilisé plutôt que le visage. Bien que cette conception mène à l'exclusion de certaines situations, par exemple, une image de si mauvaise qualité que les visages sont méconnaissables, elle propose néanmoins une approche large de la protection de l'identité : elle protège également les caractéristiques distinctives de la personne. En pratique, cette notion touche principalement les célébrités[19]. Ainsi, cette tradition juridique se caractérise par une conception dualiste de la nature des images et des droits de la personnalité en général : elle intègre des considérations à la fois patrimoniales et extrapatrimoniales[20]. C'est également l'approche retenue par la Cour suprême du Canada dans l'affaire *Aubry* c. *Éditions Vice-Versa*[21] qui, tenant compte des disparités entre l'approche du droit civil et de la common law, a opté pour la conception civiliste. Elle y affirme que le droit à l'image comprend des dimensions patrimoniales et extrapatrimoniales inhérentes au respect de la vie privée. La cour a tranché, par le fait même, que, bien que la liberté d'expression soit également un droit fondamental, celle-ci ne peut prévaloir sur le droit à l'image dans un tel contexte. En effet, ni l'expression artistique ni l'intérêt public d'être informé ne sauraient l'emporter sur l'autonomie d'une personne à disposer de son image. Encore faut-il qu'elle soit identifiable dans l'œuvre en question.

De manière générale, l'approche civile semble être la plus complète, puisqu'on peut y rattacher de nombreux droits fondamentaux déjà protégés par la Charte[22], tels que la dignité, la vie privée, l'autodétermination, l'identité personnelle et l'honneur/l'intégrité, ainsi que des droits connexes tels que le droit à l'image et l'appropriation commerciale de la personnalité[23]. Par conséquent, il pourrait bien s'agir de l'approche la mieux adaptée pour apporter une réponse efficace aux hypertrucages et offrir une plus ample stabilité juridique aux victimes qui ont été lésées.

---

18. *Id*.
19. *Id*.
20. *Id*.
21. [1998] 1 R.C.S. 591.
22. Charte, préc., note 9, art. 1, 3, 7 et 8.
23. Gert BRUGGEMEIR *et al.*, « A common core of personality protection », dans *Personality Rights in European Tort Law*, Cambridge, Cambridge University Press, 2010 (The Common Core of European Private Law), en ligne : <https://www.cambridge.org/core/books/personality-rights-in-european-tort-law> (consulté le 12 octobre 2024).

2.2 États de common law

Alors que les États membres continentaux, comme la France et l'Allemagne, accordent explicitement une protection à la représentation, les juridictions de common law, comme l'Irlande, qui suivent principalement les principes du Royaume-Uni, ne le font pas. Elles offrent toutefois une protection juridique contre les composantes dignitaires et commerciales de l'image d'une personne dans le cadre de recours en responsabilité civile. Par crainte de restreindre la liberté d'expression, cette protection n'est toutefois pas systématique : les tribunaux semblent plus réticents à accorder un droit à l'image, car « les images disent normalement la vérité »[24]. Il va sans dire que cette affirmation est aujourd'hui dépassée. Au Royaume-Uni, le système de responsabilité civile relatif aux images se divise en deux catégories : le *passing off* et l'abus de confiance. La diffamation pourrait également s'appliquer à cette question selon la situation. Si la jurisprudence récente semble élargir la portée de ces délits pour mieux s'adapter aux litiges modernes, ces doctrines gagneraient à être modernisées davantage afin de mieux protéger la vie privée des individus[25].

Au regard du droit moral, la doctrine d'abus de confiance pourrait servir de substitut à une protection explicite de la vie privée, comme l'ont démontré les affaires *Campbell* et *Douglas* au milieu des années 2000. En ajoutant les principes de « l'attente raisonnable de protection de la vie privée »[26] au premier et l'idée de reconnaître la nature hybride des photos de mariage qui ont des considérations à la fois privées et commerciales[27] au second, on s'oriente vers une meilleure protection implicite des droits de la personnalité au Royaume-Uni, sans pour autant les reconnaître textuellement[28]. De l'autre côté de cette même médaille se trouve la doctrine du *passing off*, qui pourrait protéger les composantes économiques de la représentation d'une personne, à l'instar du droit à la publicité en vigueur aux États-Unis. Les conditions pour appliquer ce délit sont toutefois assez rigides et ne trouvent conséquemment qu'une application limitée dans le contexte des hypertrucages. En effet, comme l'indique l'arrêt *Warnink*, le délit exige « une fausse déclaration faite par un commerçant dans le cadre du commerce à ses clients potentiels ou aux consommateurs finaux des biens ou services qu'il a fournis, qui

24. Michael TUGENDHAT, « Exploitation of Image Rights in the UK », dans T. SYNODINOU, préc., note 17.
25. T. SYNODINOU, préc., note 17.
26. *Campbell* c. *Mirror Group Newspapers Ltd.*, [2004] 2 AC 457 (HL).
27. *Douglas* c. *Hello*, [2007] UKHL 21.
28. T. SYNODINOU, préc., note 17.

est calculée pour nuire à l'activité ou au fonds de commerce d'un autre commerçant et qui cause un dommage réel […] »[29]. Même la trinité de *Reckitt & Colman* en matière de *passing off* (fonds de commerce, fausse déclaration, préjudice)[30] ne s'applique que peu aux hypertrucages, surtout si l'on tient compte de jurisprudences telles que *Fenty* c. *Arcadia*, dans laquelle les tribunaux anglais ont réaffirmé qu'il n'existe « pas de "droit à l'image" ou de "droit à la personnalité" qui permet à une célébrité de contrôler l'utilisation de son image »[31]. La protection des droits patrimoniaux relatifs à l'image n'est donc pas prise en compte dans ce contexte, car elle suppose généralement une concurrence, ou du moins un champ d'activités commun entre les parties[32]. Dans le cas des hypertrucages, si les victimes subissent indubitablement des dommages, les autres éléments ne sont pas aussi certains. Plutôt que de fausses déclarations, il est plus juste de parler d'appropriation illicite[33] et, bien que l'on puisse faire valoir que, dans le cas de célébrités, le fonds de commerce peut trouver application et qu'en commercialisant leur identité, le contenu hypertrucage relève de leur « domaine commun d'activités », les personnes qui choisissent de ne pas exploiter leur identité peuvent se retrouver sans recours avec la doctrine du *passing off*. Malgré une tendance jurisprudentielle récente qui s'écarte quelque peu de l'exigence du champ commun d'activité, le droit anglais, et, par extension, la common law, est généralement réticent à accorder des droits non économiques, en particulier à ceux qui ont choisi de ne pas commercialiser leur image, limitant grandement le champ d'application potentiel aux hypertrucages. En bref, les délits de common law ne sont probablement pas aussi bien adaptés que le droit civil pour s'attaquer aux hypertrucages devant les tribunaux.

3. Problèmes de compétence

Troisièmement, les droits de la personnalité n'étant pas de nature territoriale, contrairement aux droits de propriété intellectuelle, il est parfois difficile d'appliquer les règles de compétence lorsqu'une atteinte aux droits de la personnalité est invoquée. En particulier dans un contexte numérique, ces plaintes sont complexes à évaluer pour les tribunaux nationaux, autant en termes de compétence et de droit applicable que de réparations, parfois peu efficaces dans le contexte transfrontalier des questions liées à l'activité en

29. Affaire *Warnink* c. *Townend (Advocaat)*, [1979] AC 731.
30. Affaire *Reckitt & Colman Products* c. *Borden Inc.*, [1990].
31. [2013] EWHC 2310.
32. T. SYNODINOU, préc., note 17.
33. *Id*.

ligne[34]. La législation générale de l'UE en matière de compétence pour les questions extracontractuelles est codifiée dans les articles 4 et 7, paragraphe 2, du Règlement Bruxelles I bis de la directive sur la responsabilité civile des entreprises[35]. Le RGPD précise également la compétence juridictionnelle à l'article 79 lorsque l'action est intentée contre un sous-traitant ou un responsable du traitement[36]. Dans la plupart des cas, le règlement Bruxelles I bis s'applique, donc aux fins du présent article, cette disposition sera examinée nonobstant la disposition du RGPD relative à la compétence.

Il convient de préciser que, si l'article 7(2) offre une alternative au défendeur qui peut choisir de ne pas présenter sa demande à sa juridiction d'origine comme le prévoit l'article 4, il n'a pas pour but d'offrir à la partie la plus faible une protection plus forte[37]. Il vise plutôt à garantir que la juridiction compétente soit prévisible et que la sécurité juridique soit préservée[38]. Une juridiction alternative, qui serait également compétente, pourrait donc être le lieu où le dommage s'est produit, ou le lieu de l'événement à l'origine du dommage. Compte tenu de la difficulté inhérente à l'établissement de ces circonstances dans les litiges liés à l'activité en ligne, la CJUE a déclaré que l'événement causal était l'activation du processus technique affichant le contenu[39]. Dans les affaires d'hypertrucage, nous sommes donc confrontés à deux possibilités : l'activation de la technologie créant le contenu et l'activation du processus de publication de ce contenu sur une plateforme en ligne. Il est encore plus difficile d'établir le lieu du dommage dans ce type d'affaire, car il peut produire des effets dommageables pour la victime dans plusieurs endroits simultanément. En outre, considérant l'absence d'harmonisation des droits de la personnalité comme démontré précédemment, il est très probable que la protection accordée dans de telles situations varie considérablement de juridiction en juridiction. En réponse, la CJUE a déclaré dans les affaires *eDate* et *Bolagsupplysningen* que, concernant l'atteinte aux droits de la personnalité en ligne, l'interprétation de

34. Pedro De MIGUEL ASENSIO, « Protection of Reputation, Good Name and Personality Rights in Cross-Border Digital Media », (2022) 71(11) *GRUR International* 1019, en ligne : <https://doi.org/10.1093/grurint/ikac090> (consulté le 11 octobre 2024).
35. Règlement (UE) nº 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, [2012] JO L351/1, (Bruxelles I bis).
36. RGPD, préc., note 8, art. 79.
37. Affaire C-133/11 Folien Fischer et Fofitec, ECLI:EU:C:2012:664, par. 46.
38. Affaire C-523/10 Wintersteiger, ECLI:EU:C:2012:220, point 23.
39. *Id.*, par. 35-37, sur la violation des marques de commerce.

l'article 7(2) du règlement Bruxelles I bis doit être adaptée[40]. Cela donne lieu à deux concepts opposés : le critère du centre d'intérêt et l'approche mosaïque. D'abord, l'approche du centre d'intérêt permet à une personne de saisir le tribunal de sa propre juridiction (pour les personnes physiques, il s'agit le plus souvent du lieu de résidence) qui peut alors statuer sur tous les dommages causés par un contenu en ligne, quel que soit le lieu où les dommages se sont produits. L'affaire *Mittelbayerischer Verlag*[41] définit l'application de ce concept et ses limites[42]. En d'autres termes, elle confère à la juridiction nationale une compétence globale pour statuer sur une affaire transfrontalière liée à l'activité sur Internet. Ensuite, à l'opposé, on trouve l'approche controversée de la mosaïque, qui ouvre la possibilité de fragmenter le litige et d'engager des poursuites dans toute juridiction où le contenu préjudiciable est accessible, comme vu dans l'affaire *Gtflix*[43].

Évidemment, il n'existe pas de solution parfaite pour les tribunaux dans leur traitement des causes liées à l'activité en ligne, étant donné la complexité des interactions transfrontalières dans le monde numérique. Toutefois, il semblerait que le concept de centre d'intérêt puisse présenter moins d'inconvénients pour les deux parties dans les procédures concernant les hypertrucages. Il convient toutefois de noter qu'étant donné les divergences entre les juridictions quant à la protection accordée aux droits de la personnalité, une personne peut être désavantagée en fonction de son centre d'intérêt. L'approche mosaïque, quant à elle, peut, de prime abord, présenter un avantage pour le demandeur, étant donné qu'il pourrait être indemnisé dans chaque juridiction. Pourtant, en pratique, on ne peut sous-estimer la charge que représente le fait d'intenter jusqu'à 27 actions dans différents pays pour obtenir une indemnisation complète, dans l'éventualité où l'individu choisit d'éviter les tribunaux de son propre pays. En outre, pour les défendeurs, cette approche rend presque impossible de prédire dans quel État membre le contenu en ligne était disponible, ce qui va conséquemment à l'encontre du principe de sécurité juridique[44]. La multiplication actuelle des approches en termes de juridiction met en évidence la nécessité d'une harmonisation au sein de l'UE en ce qui concerne les atteintes aux droits de la personnalité.

40. P. De MIGUEL ASESIO, préc., note 34.
41. Affaire C-800/19 Mittelbayerischer Verlag, ECLI:EU:C:2021:124.
42. P. De MIGUEL ASESIO, préc., note 34.
43. Affaire C-251/20 *Gtflix Tv* c. *DR.*, [2021] ECLI:EU:C:2021:1036.
44. Tobias LUTZI, « Internet cases in EU private international law – developing a coherent approach », (2017) 66(3) *International and Comparative Law Quarterly* 687, en ligne : <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/> (consulté le 15 octobre 2024).

Effectivement, une telle harmonisation pourrait unifier le traitement de ce type de dispute à travers les tribunaux des États membres, ce qui pallierait la dichotomie des deux approches actuelles.

III. HARMONISATION

1. Le RGPD comme vecteur d'harmonisation

Compte tenu de la nécessité d'une harmonisation face aux hypertrucages dans l'UE, il est crucial d'examiner les moyens existants pour simplifier cette démarche. En effet, le RGPD pourrait bien être le vecteur par lequel les droits des personnes physiques contre les créateurs d'hypertrucages sont affirmés. En effet, comme indiqué précédemment, les IA faisant usage du *deep learning* fonctionnent sur la base du traitement de données : les technologies d'hypertrucage ne font pas exception à la règle. Par conséquent, dès lors qu'il collecte des informations sur l'apparence ou les caractéristiques vocales d'une personne choisie avec une précision telle qu'elle permet de la recréer de toutes pièces, le logiciel d'hypertrucage *traite* des données. Dû à ce traitement d'information, l'activité entre donc bel et bien dans le champ d'application du RGPD, ouvrant potentiellement la possibilité à la personne visée par le contenu d'intenter une action en justice[45]. C'est là qu'une personne peut faire valoir son droit à l'effacement ou droit à l'oubli pour que le contenu soit retiré, lorsque possible. À l'autre extrémité du champ d'application du règlement, la définition du « responsable du traitement » de l'article 1 devrait être étendue aux créateurs et admettre la possibilité d'un « contrôle conjoint » afin que la victime puisse intenter une action non seulement contre le créateur/éditeur, mais aussi contre la plateforme en vertu de l'article 77 RGPD[46]. Quant aux droits de la personnalité, ils devraient être considérés comme fondamentaux et donc inclus dans la Charte, codifiant ainsi le droit et spécifiant par le fait même son champ d'application. Cela obligerait chaque tribunal national à le reconnaître et donc à l'interpréter de la même manière. En outre, compte tenu de la nature des données utilisées pour créer l'hypertrucage, le droit à la protection des données et les droits de la personnalité devraient être interprétés comme indissociables dans le contexte des hypertrucages certes, mais également dans tout autre contexte impliquant l'utilisation de données personnelles, ce qui réaffirme la pertinence du RGPD en la matière. Il est certain que le RGPD ne peut pas être un règlement

45. Martjin VAN DER HELM, « Harmful deepfakes and the RGPD », L.L.M., Tilsburg University, 2021.
46. *Id*.

autonome pour répondre efficacement à l'industrie de l'hypertrucage ; il doit servir de fondement sur lequel d'autres législations et normes peuvent s'appuyer. En effet, les lois manquent souvent de flexibilité pour traiter de manière adéquate les questions liées aux nouvelles technologies, car celles-ci évoluent beaucoup plus rapidement que le droit. Par exemple, en 2016, lorsque le RGPD a été adopté, les hypertrucages ne pouvaient être un sujet de préoccupation, puisque le phénomène n'apparaît en ligne qu'en 2017[47]. Par conséquent, les lois de ce type sont susceptibles de rapidement devenir obsolètes et de perdre leur pertinence, d'où la nécessité de combiner les législations pour réglementer de manière adéquate les hypertrucages en créant un amalgame de lois, règlements, directives et autres, combinant plusieurs sphères du droit comme le droit pénal, la responsabilité civile, etc. Ainsi, le RGPD, d'application plus générale, combiné, entre autres, au droit pénal de chaque État membre, constitue un début prometteur pour lutter contre les hypertrucages préjudiciables malgré l'efficacité limitée du droit pénal dans les affaires liées à Internet[48].

2. Intégration des droits de la personnalité à la propriété intellectuelle

Comme indiqué précédemment, l'introduction des droits de la personnalité dans la législation de l'UE pour répondre au besoin d'harmonisation semble être la meilleure voie à suivre pour s'attaquer au phénomène des hypertrucages. Il s'agit maintenant d'imaginer comment cette modification du contexte juridique de l'UE, que ce soit par le biais du RGPD ou non, pourrait interagir avec les normes déjà existantes, telles que les droits de la propriété intellectuelle. Si la plupart des utilisations des logiciels d'hypertrucage se font de manière préjudiciable, il serait erroné de les réduire à un outil exclusivement malin utilisé pour satisfaire les fantasmes d'une poignée d'individus tordus. L'hypertrucage est également un outil créatif et, qui dit création, dit droit d'auteur. Cet article s'est principalement concentré sur les inconvénients des technologies d'hypertrucage, mais leur potentiel de résultats positifs ne peut être négligé. Nombreux sont ceux qui ont vanté les mérites de cette technologie en tant que formidable outil pédagogique, par exemple pour la reconstitution d'événements histo-

47. Organisation for Social Media Safety, « Deepfake Technology », en ligne : <https://www.socialmediasafety.org/advocacy/deepfake-technology/> (consulté le 10 janvier 2025).
48. M. VAN DER HELM, préc., note 45

riques, les nouvelles possibilités offertes en marketing[49], les objectifs d'accessibilité[50] et plus encore. Cette utilisation bénigne devrait donc également être réglementée par la propriété intellectuelle, plus particulièrement par le droit d'auteur.

Il a été mentionné que l'approche typiquement civiliste du droit de la personnalité est la plus compatible avec l'état actuel de la propriété intellectuelle. En effet, à l'instar du droit d'auteur, l'approche du droit civil reconnaît les composantes dualistes des droits de la personnalité : les droits patrimoniaux et extrapatrimoniaux. Elle se conjugue ainsi parfaitement avec les droits économiques et moraux associés au droit d'auteur[51]. Par exemple, le droit à l'intégrité est un droit commun au droit d'auteur et aux droits de la personnalité, et, bien qu'il soit généralement attribué à l'auteur plutôt qu'à l'objet de la protection, dans les cas d'hypertrucage, il ne serait sans doute pas invraisemblable d'étendre la protection à l'objet, c'est-à-dire à la personne représentée par l'hypertrucage, comme le permet la conception civile du droit à l'image. Le droit civil et la propriété intellectuelle adhèrent tous deux à une approche hégélienne de la personne[52], contrairement à l'approche américaine, par exemple, qui, en qualifiant leur doctrine de droits de publicité, adopte une position plus utilitariste. Ce traitement similaire des droits s'avère utile dans les litiges opposant les droits d'auteur aux droits de la personnalité, lorsque les tribunaux doivent balancer les intérêts des parties avec d'autres droits fondamentaux en cause. Il devient alors plus facile pour les cours d'évaluer ces disputes en « comparant des pommes avec des pommes ». En général, le consentement est l'élément clef en la matière et fait pencher la balance en faveur des droits de la personnalité par rapport au droit d'auteur et à la liberté artistique[53]. Aux fins de cet article, il convient de noter que l'accent a été mis sur les personnes physiques vivantes, car les droits de la personnalité ne s'appliquent pas aux personnes décédées, ce qui constitue un tout autre débat doctrinal. Dans les cas d'hypertrucages pornographiques, il est évident que les droits de la personnalité devraient prévaloir sur la soi-disant liberté artistique d'un auteur qui saisit le visage d'une

49. Jan KIETZMANN et Adam J. MILLS, « Deepfakes: perspectives on the future "reality" of advertising and branding », (2021) 40(3) *International J of Advertising* 473.
50. Chandra KISHOR PANDY *et al.*, « Deepfakes: When to Use It », (2021) 10th International Conference on System Modeling & Advancement in Research Trends (SMART).
51. K. TYAGI, préc., note 5.
52. *Id*.
53. T. SYNODINOU, préc., note 17.

victime de son choix sur un corps pour la voir accomplir des actes sexuels. Toutefois, lorsque l'hypertrucage est utilisé à des fins humoristiques ou satiriques, il se peut que l'on ne puisse pas invoquer une atteinte aux droits de la personnalité. L'affaire *Vereinigung Bidlender Kunstler* portait sur un homme politique figurant sur une œuvre satirique qui a tenté de faire valoir son droit à la personnalité, cet argument a été rejeté par la Cour européenne des droits de l'homme, qui a plutôt statué en faveur de l'artiste au nom de la liberté d'expression prévue à l'article 10 de la *Convention européenne des droits de l'homme*[54]. Il s'agit donc d'une question qui reste à traiter au cas par cas et qui peut être assortie d'exceptions similaires à celles prévues pour la protection du droit d'auteur. Toutefois, cette question de peser certains droits par rapport à d'autres illustre le fait que les droits de la personnalité ne sont pas absolus et ne devraient pas l'être.

IV. CONCLUSION

En conclusion, si l'on considère le contexte juridique actuel, il est évident que la législation de l'UE n'est pas suffisamment précise pour traiter des technologies d'hypertrucage, laissant ainsi à chaque État membre le soin d'appliquer ses propres recours extracontractuels. Cela laisse place à une insécurité juridique substantielle et à une protection inégale à travers l'UE. Il est donc nécessaire de procéder à une harmonisation pour résoudre ces problèmes en introduisant des droits de la personnalité en droit européen. Comme précédemment démontré, cette approche semble être la meilleure piste de solution à ce jour. Le RGPD pourrait notamment préciser son champ d'application en matière d'atteinte aux droits de la personnalité en offrant des voies de recours claires aux victimes d'hypertrucage préjudiciables. L'harmonisation des droits de la personnalité permettrait également aux tribunaux de mieux traiter les plaintes liées aux hypertrucages dans le cadre des litiges opposant les droits du créateur en propriété intellectuelle et de la victime, étant donné que le droit d'auteur et de la personnalité découlent tous deux d'une conception similaire des droits à l'image, ce qui uniformiserait les courants jurisprudentiels des tribunaux autant au niveau national que de l'UE. Avec le rythme soutenu auquel la technologie évolue, il est néanmoins primordial pour les autorités législatives de développer des méthodes innovantes pour que le droit puisse suivre la cadence du monde numérique au-delà des normes statutaires qui risquent de devenir obsolètes au fil du temps. Le cas des hypertrucages ne marque qu'un début aux lacunes

54. Affaire *Vereinigung Bildender Künstler* c. *Autriche*, [2007] 68354/01, par. 38.

du droit par rapport à l'innovation technologique et à la protection de la vie privée, non pas une fin.

BIBLIOGRAPHIE

Sources primaires

Législation

Charte des droits fondamentaux de l'Union européenne, [2012] JO C326/391, art. 8(1).

Règlement (UE) nº 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, [2012] JO L351/1 (règlement Bruxelles Ia).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), [2016] JO L 119/1.

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées en matière d'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (Loi sur l'intelligence artificielle), art. 3(60) (Loi sur l'IA).

Traité sur le fonctionnement de l'Union européenne, [2012] JO C326/47, art. 16 (TFUE).

Jurisprudence

Affaire C-133/11 *Folien Fischer et Fofitec*, ECLI:EU:C:2012:664, par. 46.

Affaire C-251/20 *Gtflix Tv* c. *DR.*, [2021] ECLI:EU:C:2021:1036.

Affaire C-523/10 *Wintersteiger*, ECLI:EU:C:2012:220, point 23.

Affaire C-800/19 *Mittelbayerischer Verlag*, ECLI:EU:C:2021:124.

Affaire *Aubry* c. *Éditions Vice-Versa*, [1998] 1 R.C.S. 59.

Affaire *Campbell* c. *Mirror Group Newspapers Ltd*., [2004] 2 AC 457 (HL).

Affaire *Douglas* c. *Hello*, [2007] UKHL 21.

Affaire *Fenty* c. *Arcadia*, [2013] EWHC 2310.

Affaire *Warnink* c. *Townend (Advocaat)*, [1979] AC 731.

Affaire *Reckitt & Colman Products* c. *Borden Inc.*, [1990].

Affaire *Vereinigung Bildender Künstler* c. *Autriche*, [2007] 68354/01, par. 38.

Sources secondaires

BRIEGER A.R., « Empowerment or exploitation: A qualitative analysis of online feminist communities' discussions of deepfake pornography » (Master, Uppsala Universitet 2024).

BRUGGEMEIR G. *et al.*, « A common core of personality protection », dans *Personality Rights in European Tort Law*, Cambridge, Cambridge University Press, 2010 (The Common Core of European Private Law). <https://www.cambridge.org/core/books/personality-rights-in-european-tort-law> (consulté le 12 octobre 2024).

DE MIGUEL ASENSIO P., « Protection of Reputation, Good Name and Personality Rights in Cross-Border Digital Media », (2022) 71(11) *GRUR International* 1019, en ligne : <https://doi.org/10.1093/grurint/ikac090> (consulté le 11 octobre 2024).

KIETZMANN J. et MILLS A.J., « Deepfakes: perspectives on the future "reality" of advertising and branding », (2021) 40(3) *International J of Advertising* 473, en ligne : <https://doi.org/10.1080/02650487.2020.1834211> (consulté le 12 octobre 2024).

LUTZI T., « Internet cases in EU private international law-developing a coherent approach », (2017) 66(3) *International and Comparative Law Quarterly* 687, en ligne : <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/> (consulté le 15 octobre 2024).

MANIA K., « Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study », (2024) 25(1) *Trauma, Violence & Abuse* 117, en ligne : <https://journals.sagepub.com> (consulté le 11 octobre 2024).

Organisation for Social Media Safety, « Deepfake Technology », en ligne : <https://www.socialmediasafety.org/advocacy/deepfake-technology/> (consulté le 10 janvier 2025).

PANDY C.K. *et al.*, « Deepfakes: When to Use It », (2021) 10th International Conference on System Modeling & Advancement in Research Trends (SMART), en ligne : <https://ieeexplore.ieee.org/document/9676297> (consulté le 12 janvier 2025).

RINI R. et COHEN L., « Deepfakes, Deep Harms », (2022) 22(2) *Journal of Ethics and Social Philosophy* 143, en ligne : < https://doi.org/io.z65s6/jesp.vzziz.16z8> (consulté le 13 octobre 2024).

SYNODINOU T., « Image Right and Copyright Law in Europe: Divergences et convergences », (2014) 3 *Laws* 181, en ligne : <https://www.mdpi.com/journal/laws> (consulté le 12 octobre 2024).

Security Hero, « 2023 State of Deepfakes: Realities, Threats, and Impact », (Security Hero, 2023), en ligne : <https://www.securityhero.io/state-of-deepfakes> (consulté le 14 octobre 2024).

TYAGI K., « Deepfakes, Copyright & Personality Rights: An Interdisciplinary Perspective », (document de conférence, avril 2022), en ligne : <https://www.researchgate.net/publication/359711219> (consulté le 11 octobre 2024).

VAN DER HELM M.J., « Harmful deepfakes and the RGPD » (L.L.M., Université de Tilsburg 2021).