

# Un deepfake utilisant l'image d'un salarié peut-il constituer une infraction ?

## Réponse courte

Oui, un **deepfake** utilisant l'image d'un salarié peut constituer plusieurs infractions cumulatives au Luxembourg. Sur le plan civil, il viole le **droit à l'image** protégé par l'article 9 du Code civil, ouvrant droit à des dommages-intérêts. Sur le plan pénal, il peut qualifier une **usurpation d'identité**, une atteinte à l'honneur, une diffamation ou un faux selon le contenu. Au titre du RGPD, l'image d'une personne identifiable est une **donnée à caractère personnel** et, lorsqu'elle sert à identifier ou authentifier, relève des **données biométriques** visées à l'article 9 RGPD, dont le traitement est en principe interdit.

Depuis l'entrée en vigueur progressive du **Règlement (UE) 2024/1689 (AI Act)**, les contenus générés ou manipulés par IA doivent faire l'objet d'un **étiquetage clair** indiquant leur caractère synthétique. L'entreprise victime ou le salarié concerné peuvent saisir le **tribunal d'arrondissement** en référé pour obtenir le retrait du contenu, déposer plainte auprès du parquet et notifier la **CNPD** en cas de violation de données personnelles. L'accompagnement par le **service juridique** et la **délégation du personnel** est recommandé.

## Définition

Un **deepfake** est un contenu audio, vidéo ou image **synthétique ou manipulé** produit par des techniques d'**intelligence artificielle générative**, représentant une personne réelle dans une situation qu'elle n'a pas vécue ou lui faisant tenir des propos qu'elle n'a pas tenus. Juridiquement, il combine plusieurs atteintes potentielles : atteinte au **droit à l'image**, usurpation d'identité, traitement illicite de **données biométriques**, diffamation ou faux.

Le **droit à l'image** est un attribut de la personnalité reconnu par l'article 9 du Code civil luxembourgeois, qui protège la vie privée. Toute reproduction ou diffusion de l'image d'une personne identifiable sans son consentement est illicite, sauf exception légitime (information, débat public, caricature). L'**AI Act** ajoute une obligation spécifique de **transparence** : les fournisseurs et déployeurs de systèmes d'IA générant des deepfakes doivent rendre visible leur nature artificielle.

## Conditions d'exercice

La qualification d'un deepfake dépend de critères cumulatifs évalués au cas par cas.

| Critère                 | Règle                                                     |
|-------------------------|-----------------------------------------------------------|
| Identifiabilité         | La personne doit être reconnaissable sur le contenu       |
| Absence de consentement | Pas d'autorisation écrite préalable du salarié            |
| Intention ou effet      | Tromperie, nuisance, atteinte à l'honneur ou à la dignité |
| Diffusion               | Publication publique ou partage à un tiers                |
| Contexte professionnel  | Lien avec l'activité, les collègues ou l'employeur        |
| Traitement de données   | Image comme donnée personnelle voire biométrique          |

## Modalités pratiques

La victime et l'entreprise disposent de plusieurs voies d'action à engager sans délai.

| Étape                  | Modalité                                                  |
|------------------------|-----------------------------------------------------------|
| Constatation           | Capture d'écran, constat d'huissier, horodatage           |
| Signalement plateforme | Demande de retrait via procédure officielle du réseau     |
| Plainte pénale         | Dépôt au parquet pour usurpation, diffamation ou faux     |
| Action civile          | Référé devant le tribunal d'arrondissement pour retrait   |
| Notification CNPD      | Si traitement illicite de données biométriques            |
| Information interne    | Délégation du personnel, soutien psychologique du salarié |

## Pratiques et recommandations

Il est fortement recommandé de traiter un deepfake comme un **incident grave** combinant atteinte aux personnes et risque réputationnel pour l'entreprise. La **réactivité** est essentielle car la viralité des contenus synthétiques rend le préjudice exponentiel dans les premières heures. L'employeur doit conserver toutes les **preuves numériques** (URL, métadonnées, captures horodatées) et mandater un huissier pour un constat opposable en justice, tout en garantissant la **protection du salarié** victime.

Le **service juridique** doit coordonner les actions civiles et pénales en parallèle, privilégiant le **référé-heure** devant le tribunal d'arrondissement lorsque le préjudice est imminent. La **CNPD** doit être notifiée dans les 72 heures lorsque le deepfake implique un traitement de données biométriques, conformément à l'article 33 du RGPD. Enfin, une **sensibilisation** interne sur les risques liés à l'IA générative et une charte encadrant l'usage professionnel de l'image des salariés constituent des mesures préventives incontournables.

## Cadre juridique

| Référence                         | Objet                                             |
|-----------------------------------|---------------------------------------------------|
| Art. 9 du Code civil              | Droit au respect de la vie privée et à l'image    |
| Code pénal luxembourgeois         | Usurpation d'identité, diffamation, faux          |
| Art. 9 RGPD                       | Interdiction de principe des données biométriques |
| Art. 33 RGPD                      | Notification de violation à la CNPD               |
| Règlement (UE) 2016/679 (RGPD)    | Protection des données à caractère personnel      |
| Loi du 1er août 2018              | Transposition luxembourgeoise du RGPD             |
| Règlement (UE) 2024/1689 (AI Act) | Obligations de transparence des deepfakes         |
| Art. 11 de la Constitution        | Libertés publiques et dignité humaine             |

Le deepfake combine plusieurs qualifications juridiques, ce qui permet des actions cumulatives au civil, au pénal et au titre du RGPD. L'obligation de transparence de l'AI Act renforce les recours contre les contenus non étiquetés. Une réaction rapide et documentée conditionne l'effectivité du retrait et la preuve du préjudice.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.