Préjudice moral de la cyber malveillance et de la surveillance

Le préjudice moral lié à la cybermalveillance (cyberattaques, usurpation d'identité, cyberharcèlement, diffusion de contenus humiliants, etc.) et à la surveillance illicite (intrusion dans la vie privée, cybersurveillance abusive, fuites de données) est bien reconnu en droit français, tant pour les personnes physiques que (dans une moindre mesure) pour les personnes morales.

Préjudice moral : définition et reconnaissance

Le préjudice moral correspond à l'atteinte aux droits de la personnalité (dignité, intimité, honneur, image de soi, tranquillité d'esprit). Il se manifeste souvent par :

Angoisse, stress, anxiété, troubles du sommeil

Sentiment d'humiliation ou de perte de contrôle sur sa vie privée

Atteinte à la réputation ou à l'estime de soi

Sentiment d'insécurité durable

En matière numérique, la jurisprudence et la doctrine considèrent de plus en plus que la simple violation de données personnelles ou la crainte fondée d'une utilisation abusive (chantage, usurpation, harcèlement ultérieur) suffit à caractériser un préjudice moral indemnisable — sans qu'il faille nécessairement prouver une utilisation effective et dommageable des données (influence importante de la CJUE, notamment arrêt du 4 mai 2023, C-300/21, et arrêts nationaux qui suivent cette ligne).

Principaux cas en cybermalveillance

Cyberharcèlement (art. 222-33-2-2 Code pénal) → forme aggravée de harcèlement moral quand il est commis en ligne. Préjudice moral très fréquemment indemnisé (angoisses, dépression, retrait social, parfois suicidalité). Les tribunaux accordent souvent plusieurs milliers d'euros selon la gravité et la durée.

Atteinte à la vie privée (art. 226-1 et s. Code pénal) → diffusion non consentie d'images intimes (revenge porn), surveillance intrusive, doxxing. Préjudice moral systématiquement retenu.

Usurpation d'identité / Phishing massif → au-delà du préjudice financier, le sentiment de violation de l'intimité et de perte d'identité génère un préjudice moral reconnu.

Fuites de données / Ransomware avec menace de publication → pour les particuliers, la crainte d'exploitation des données (données de santé, orientation sexuelle, données bancaires…) est indemnisable).

Cas spécifiques de surveillance illicite:

Logiciels espions, contrôle excessif des mails/écrans sans information préalable ni proportionnalité) :Préjudice moral fréquent (sentiment d'être épié, perte de confiance, stress).

Surveillance étatique (??)ou privée massive (??)(si illégale) → peut générer un préjudice moral via le sentiment d'atteinte à la liberté et à l'intimité (RGPD art. 82 + jurisprudence CJUE). TERREUR.

Stalking numérique / Géolocalisation intrusive → préjudice moral important (peur permanente, modification des comportements).

Plainte pénale → au commissariat, gendarmerie ou par plainte en ligne (pré-plainte). Permet poursuites + constitution de partie civile pour demander réparation.

Action civile → devant tribunal judiciaire (dommages-intérêts pour préjudice moral + matériel).

Saisine CNIL → si violation RGPD (fuite de données, surveillance illicite) → peut aboutir à sanction + faciliter indemnisation.

Aide aux victimes → 116 006 (France Victimes), plateforme 3018 (cyberharcèlement mineurs), cybermalveillance.gouv.fr.

Assurance → certaines contrats habitation ou cyber incluent la couverture du préjudice moral.

Le droit évolue rapidement dans ce domaine : la combinaison RGPD + jurisprudence européenne facilite de plus en plus la reconnaissance d'un préjudice moral en cas de surveillance intrusive.