# Modération des contenus illicites en ligne

## Opérations et protection des professionnels

**CONTENUS TERRORISTES ET D'EXPLOITATION SEXUELLE DE MINEURS**

## Octobre 2023

Ce document est la 3e édition proposée par Point de Contact de son Livre Blanc relatif au traitement des signalements de contenus illicites et à la protection des professionnels du secteur Trust & Safety.

Déjà en 2019, notre association proposait un successeur au Guide d'Usage pour la Lutte Contre la Pédopornographie, rédigé en 2014 par le service abuse de Gandi.net. Pour cette édition, Point de Contact a mis un point d'honneur à constituer un comité de rédaction rassemblant des experts de tous horizons, comprenant notamment plateformes privées, hébergeurs, autorités publiques, médecins et magistrats. Nous tenons par ailleurs à adresser nos remerciements à l'ensemble des personnes constituant ce comité, leur dévouement et leur implication dans ce projet auront été déterminants.

Cette nouvelle actualisation du texte par Point de Contact s'inscrit dans la dynamique de responsabilisation des acteurs du monde numérique, tant sur le plan de la régulation des contenus et des comportements en ligne que sur celui de la prise en charge des besoins spécifiques de ces corps de métier. La sortie de cette édition intervient à l'automne 2023, au cœur du processus d'entrée en vigueur du Digital Services Act à l'échelle européenne.

POINT
DE
CONTACT
.NET

# Sommaire

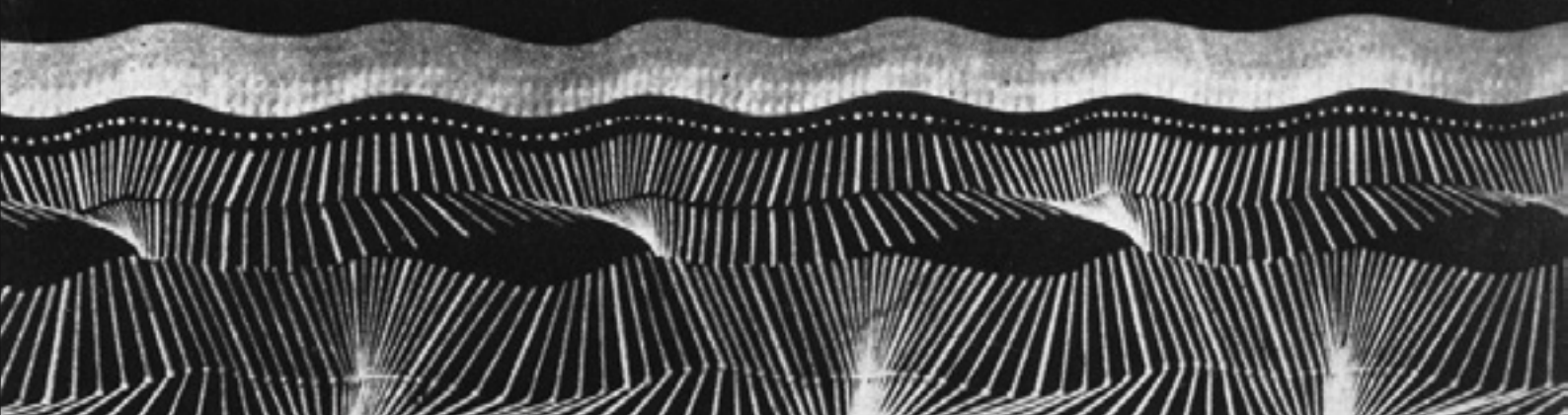
# Mot du Président de Point de Contact

## Le livre blanc d'une communauté de professionnels en mouvement

Au tournant des années 2010, un petit groupe de professionnels s'était constitué et se réunissait de manière informelle, à l'écart de leurs hiérarchies, pour échanger sur leur métier si particulier : le traitement des contenus de « pornographie enfantine » comme on l'appelait à l'époque. Leur métier n'avait pas de nom, il s'inscrivait tout au plus dans la lutte contre la cybercriminalité, certains appartenaient à des équipes « abuse » chez les hébergeurs ou les fournisseurs d'accès. Faute de cadre juridique et sociétal bien établi, il fallait se serrer les coudes, définir les bonnes pratiques opérationnelles, aborder – timidement – la question difficile de l'impact psychologique de l'exposition répétée à des contenus choquants. Dans le premier « guide d'usage » qui fut publié en 2014, un titre de section accroche le regard : « Vous n'êtes pas seuls ».

Ce nouveau livre blanc est la photographie d'une communauté professionnelle en mouvement. Il capture l'époque à la manière d'une photographie d'Étienne-Jules Marey : on voit le sujet avancer. A partir du « guide d'usage » de 2014, devenu « livre blanc » en 2019, à cette nouvelle édition de 2023, l'évolution est frappante. La dimension pratique reste le socle, mais les mentalités évoluent et s'enhardissent. Le terme pédocriminalité s'impose enfin (à défaut d'être dans la loi), la thématique psy explose (une seule occurrence dans le guide de 2014, quarante-six dans le premier livre blanc, soixante-dix dans cette version), la philosophie fait son entrée.

Enfin, la diversité des professionnels, dans l'industrie, les associations et le secteur public et judiciaire se regroupe sous un nouveau vocable, qui a le mérite d'exister à défaut d'avoir sa traduction française, celui de la Trust & Safety. Dans le monde, les professionnels exposés à des contenus choquants se comptent en centaines de milliers, depuis les équipes opérationnelles dans l'industrie jusqu'aux autorités judiciaires. La tâche devant nous est immense, et 2024 s'annonce comme le début d'une nouvelle phase pour la régulation du numérique, des plateformes aux régulateurs en passant par la société civile. Dans cet environnement dynamique, ce livre blanc se veut fidèle à l'esprit confraternel des sept pionniers de 2014 et ambitionne d'être une source d'inspiration et d'orientation fédératrice pour cette grande communauté qui se forme sous nos yeux.



# Introduction

## Objectifs et enjeux

**Finalités.** L'objet de ce livre blanc est de créer un socle commun de bonnes pratiques professionnelles en matière de traitement opérationnel des contenus choquants et potentiellement illicites qui mettent en jeu l'équilibre psychologique des professionnels et, par ricochet, leur santé physique.

**Audience.** Ce document s'adresse à une pluralité de structures intervenant dans la diffusion et la régulation de ces contenus. Il a ainsi vocation à intéresser l'ensemble des professionnels susceptibles d'être confrontés à ces contenus choquants qu'ils soient issus du secteur privé (modérateurs des fournisseurs d'accès, hébergeurs, plateformes et tout autre opérateur légalement reconnu) et du secteur public (en particulier la chaîne pénale, des enquêteurs aux magistrats, des greffiers aux avocats ...). Les thérapeutes se reconnaîtront également dans cette définition.

**Champ d'application.** Les contenus choquants visés dans ce livre blanc relèvent de deux catégories distinctes : les images ou représentations de mineurs présentant un caractère sexuel[1] et les contenus terroristes[2]. Certaines des bonnes pratiques présentées dans ce livre blanc pourront aussi s'appliquer à d'autres types de contenus choquants.

**Champ géographique.** Bien que les typologies de contenus abordées dans ce document – ainsi que les bonnes pratiques professionnelles dans leur traitement – n'ont pas de rattachement géographique et peuvent se trouver dans tous les pays du monde, le périmètre de ce livre blanc se limite juridiquement à la France. De même, les processus de signalements mentionnés dans ce document sont relatifs spécifiquement aux autorités françaises. Cependant, les lecteurs, francophones ou non, qui souhaiteraient mettre en place des processus similaires pour d'autres pays pourront se tourner vers leurs autorités compétentes afin de connaître les procédés et méthodes locales.

**Accroissement des menaces.** Alors que la diffusion et l'accessibilité de ces contenus connaissent depuis les années 1990 une croissance continue, force est de constater que cette progression s'est encore accélérée depuis 2010[3], avec le développement, tant des appareils connectés (smartphones, tablettes, téléviseurs connectés, consoles de jeux vidéo), que des réseaux à haut débit fixes et mobiles.

**Renforcement de la lutte.** Les effectifs des personnels assignés au traitement de ces contenus ont eux aussi drastiquement augmenté, justement en raison de l'accroissement de la volumétrie, de sorte que les professions liées à ce secteur connaissent aujourd'hui un essor sans précédent. Les petites entreprises, autant que les grandes, se voient de plus en plus contraintes de se doter de services consacrés

1 Article 227-23 du Code pénal français
2 Article 421-2-5 du Code pénal français et Règlement (UE) 2021/784 du Parlement Européen et du Conseil, du 29 avril 2021, relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne
3 En 2015, la base de données ICCAM du réseau INHOPE recensait 38 448 contenus qualifiés d'exploitation sexuelle de mineurs. En 2020, la même qualification avait été appliquée à 492 961 contenus, soit une hausse d'environ 1 195%.

à la modération de contenus. Cependant, malgré un recours grandissant à des outils technologiques (automatisation, intelligence artificielle), le traitement et l'analyse précise de ce type de contenus maintiennent indispensable l'intervention humaine.

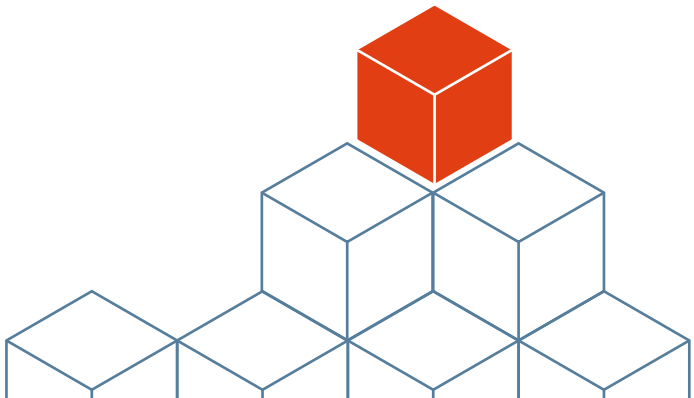
**Périmètre.** La protection des victimes visibles dans ces contenus, ainsi que la protection des personnes confrontées à ces derniers, appellent l'intervention de professionnels. C'est pourquoi il est indispensable d'apporter un socle commun de bonnes pratiques pour renforcer l'efficacité des circuits de signalement. Les contenus choquants sont de nature à affecter tout individu y étant confronté, qu'il y soit exposé régulièrement ou ponctuellement. Parce que certains personnels constituent une première ligne de défense essentielle, ce livre blanc entend contribuer à reconnaître leur rôle et la nécessité de leur garantir un cadre de travail et un soutien psychologique adapté.

# Terminologie

**Renoncement au terme "pédopornographie".** Le comité de rédaction de ce livre blanc souligne la nécessité d'abandonner l'usage des termes « pédopornographie » ou « pornographie enfantine », pour leur préférer un vocabulaire mettant l'accent sur le caractère criminel des activités dont il est question. L'association de l'enfant à la pornographie invisibilise le statut des victimes d'exploitation et d'abus sexuels d'enfants. La pornographie ne devrait renvoyer, quant à elle, qu'aux seules activités sexuelles consenties entre adultes.

**Emploi du terme pédocriminalité.** Le champ lexical utilisé au sein de ce document sera donc celui de la pédocriminalité, ce qui permettra d'inclure les termes de matériel ou de contenus d'exploitation sexuelle de mineurs. La terminologie de contenus d'abus sexuels sur mineurs, traduction de la qualification "Child Sexual Abuse Material" (CSAM), pourra occasionnellement apparaître, afin de tenir compte de la nomenclature internationale. Ce choix a vocation à souligner le fait que l'enfant ou l'adolescent est victime, et non pas un acteur consentant et/ou responsable des actes représentés.

**Sens et portée.** Alors même que les mots « pédopornographie » ou « contenus pédopornographiques » sont encore utilisés par la législation française et sont connus du grand public, il apparaît important de se livrer à cette distinction sémantique. Ce choix délibéré se place ainsi en soutien des attentes émanant de la société civile et du monde académique dans la perspective de rendre compte, par les mots et leur sens, de réalités le plus souvent extrêmement violentes.



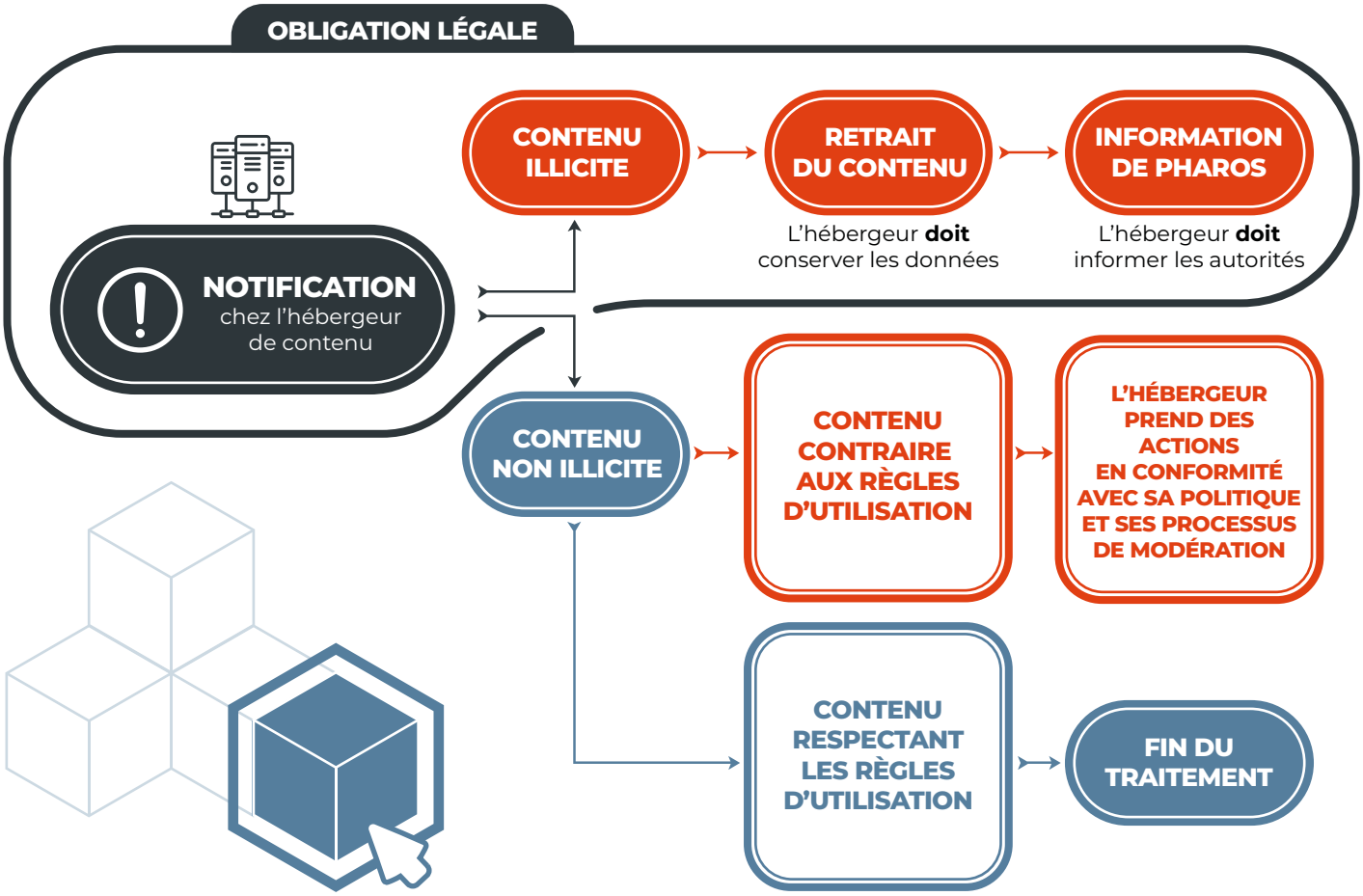
# PARTIE I

# LE SIGNALEMENT

**Contenus illicites.** La loi française pour la confiance dans l'économie numérique (LCEN)[4] et désormais le Digital Services Act (DSA)[5] européen disposent que tous les hébergeurs, personnes physiques ou morales, doivent concourir à la lutte contre les contenus et activités illicites. Une importance particulière est accordée aux contenus terroristes[6], parmi lesquels les infractions de provocation à la commission d'actes de terrorisme et leur apologie, ainsi qu'aux contenus pédocriminels.

**Régime.** La principale obligation positive issue de ces textes réside dans la mise en place de mécanismes à destination de particuliers et d'entités, visibles et faciles d'accès et d'utilisation, permettant de signaler aux hébergeurs la présence de contenus illicites sur leurs services (I). Dans l'éventualité où, après qualification (II), le contenu est considéré illicite, il naît une nouvelle série d'obligations qui consiste à retirer ou rendre l'accès au contenu impossible et d'informer les autorités compétentes de leur présence (III).

4 Article 6, I., alinéa 7 de la Loi n° 2004-575 pour la confiance dans l'économie numérique, 21 juin 2004
5 Article 16 du Règlement (UE) 2022/2065 du Parlement Européen et du Conseil, 19 Octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Règlement sur les services numériques, RSN ou DSA)
6 Règlement (UE) relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *op.cit.*




# I – L'élaboration du dispositif de signalement

## A – La mise en place d'un mécanisme de signalement

**Obligation légale.** La première obligation est celle de mettre à disposition du public un moyen de signalement accessible et dont la procédure doit pouvoir être intégralement poursuivie en ligne, en quelques clics. Pour ce faire, il convient de mettre en place un dispositif spécifiquement dédié, facilement identifiable, simple d'utilisation et gratuit.

**Diversité des mécanismes de notification.** Un dispositif de signalement se matérialise le plus souvent par un formulaire dédié, ou par une adresse mail de type abuse@exemple.tld. Pour les contenus édités sur les plateformes et réseaux sociaux, l'internaute devrait pouvoir les signaler à tout moment lors de sa navigation.

**Formulaire de signalement.** Le recours au formulaire présente plusieurs avantages, qu'il s'agisse de guider l'utilisateur dans sa démarche ou de fournir aux analystes

de contenus des données permettant de contextualiser le signalement. À ce titre, il est important de trouver un équilibre convenable entre deux impératifs : l'efficacité opérationnelle du traitement et l'opportunité de disposer d'éléments de contexte – qui constitue aussi une revendication importante de la part de la société civile. L'exigence de simplicité du processus de signalement invite notamment à prendre en compte les situations où des individus mineurs souhaitent soumettre de telles notifications.

**Modalités du signalement.** Enfin, les contenus accessibles publiquement devraient pouvoir être signalés sans création de compte préalable[7], par exemple, par le biais du centre d'aide ou d'assistance de l'hébergeur. Il est en effet indispensable d'offrir la possibilité à tout individu de soumettre des demandes de retrait, même sans communiquer de moyens d'identification tels qu'une adresse e-mail. Toutefois, dans le cas où l'internaute a fourni ses coordonnées électroniques, l'hébergeur est tenu d'accuser réception du signalement dans les meilleurs délais[8].

## B – L'accueil technique des signalements

**Canal exclusif.** Il est fondamental que le canal de signalement soit réservé uniquement à cet usage afin de pouvoir isoler ces informations des autres échanges (demandes adressées au service commercial, plaintes de consommateurs, demandes de renseignements, etc.) La réception des signalements de contenus potentiellement illicites doit en effet être réservée aux personnels habilités à les traiter.

**Étanchéité des bases de données.** Les fichiers concernés doivent être traités dans un environnement technique clos, qui ne permet pas le partage, la reproduction, ou l'exportation en dehors dudit environnement. Par exemple, il ne doit idéalement pas être possible de télécharger des images depuis le logiciel de traitement des signalements, ni d'envoyer les fichiers par mail ou tout autre canal de communication.

**Prévention de l'exposition accidentelle.** De même, les autres salariés non affectés à leur analyse ne doivent pas y être exposés. Traiter ce type de contenus nécessite impérativement le consentement du salarié, et ne doit en aucun cas être imposé arbitrairement. C'est pourquoi il est important de prévenir matériellement toute exposition accidentelle. Des recommandations spécifiques, en lien notamment avec la protection des professionnels, seront proposées tout au long de ce document.

**Diversité des risques.** Si la prévention contre une exposition visuelle à ce type de contenus doit constituer une priorité, il est également conseillé de ne pas les évoquer verbalement avec un entourage professionnel non formé. Certaines descriptions graphiques de contenus rencontrés peuvent en elles-mêmes heurter. Il est préférable de réserver ces échanges aux espaces y étant dédiés – lors d'un entretien psychologique par exemple.

7 Article 16, §1 du Règlement (UE) relatif à un marché unique des services numériques (DSA), *op. cit.*
8 Article 16, §4 du Règlement (UE) relatif à un marché unique des services numériques (DSA), *op. cit.*

# II – La qualification des contenus

## A – Qualifier un contenu pédocriminel

**Droit applicable.** L'enregistrement en vue de diffuser, la détention, la transmission, la mise en ligne, ou la seule consultation régulière de contenus pédocriminels sont incriminés par le Code pénal français. A fortiori, si l'individu enregistré dans ces images a moins de quinze ans, il n'est pas nécessaire de déceler une intention de diffusion, la simple capture de telles images est une infraction[9].

**Contenus sexuels.** Pour être qualifié d'illicite, le contenu observé doit avoir un caractère sexuel. La loi française n'offre pas de définition précise de ce qu'est une image ou une représentation d'un mineur à caractère sexuel, mais d'autres sources[10] peuvent apporter un éclairage à cette question. La directive européenne relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[11] offre des précisions en ce sens. Un contenu pédocriminel se rapporte ainsi à toute représentation[12] visuelle d'un mineur – ou d'un individu paraissant mineur – se livrant à un comportement sexuellement explicite, réel ou simulé[13], ou toute représentation de ses organes sexuels, à des fins principalement sexuelles.

**Évaluation de la minorité.** Des contenus sont qualifiés de pédocriminels lorsqu'ils mettent en scène des mineurs, c'est-à-dire des personnes de moins de 18 ans. Si la détermination de la minorité d'un enfant ne pose généralement pas de difficultés, la distinction entre une personne mineure adolescente et une personne adulte n'est pas toujours évidente[14].

**Apparence de minorité.** Le dernier alinéa de l'article 227-23 du Code pénal prévoit en ce sens que tombent aussi sous le coup de la loi les images de personnes dont l'aspect physique est celui d'un mineur. Ce qui est visé ici est l'apparence de minorité. Dans le doute sur l'âge d'une personne, il est ainsi conseillé d'effectuer un signalement.

**Analyse contextuelle.** Le caractère sexuel exclut ainsi a priori les images de nudisme ou de naturisme, ainsi que les images d'enfants nus dans un contexte non sexualisé. En revanche, cela inclut toutes les images d'enfants nus, ou habillés, dont l'analyse du contexte, les caractéristiques de la prise de vue, la focalisation sur certaines parties du corps, la posture adoptée par l'enfant, et les éventuels accessoires ajoutés peuvent orienter la qualification. Ainsi, en tenant compte du contexte, une image représentant

9 Article 227-23 du Code pénal français *op.cit.*
10 Plusieurs sources, référencées en annexe, proposent des définitions d'un contenu à caractère pédocriminel.
11 Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie
12 *Ibid*, Article 2, c) iv) : le mot "représentation" concerne aussi bien des enregistrements que des images, dessins ou autres représentations fictives.
13 *Ibid*, Article 2, c), i), ii), iii)
14 Pour plus d'informations : de nombreux organismes scientifiques ont pu élaborer des classifications afin d'évaluer les différents stades du développement pubertaire. Le réseau international INHOPE, par exemple, met à disposition de ses analystes professionnels des manuels permettant de détecter plus facilement des indicateurs de puberté.

un enfant nu peut être licite, alors que celle mettant en scène un enfant habillé peut être illicite.

**Contenus virtuels.** La législation française vise indistinctement les contenus réels ou virtuels. Les dessins, photomontages ou hypertrucages (“*deepfakes*”) générés par une intelligence artificielle constituent donc eux aussi des contenus illicites. La loi transposant les dispositions du Digital Services Act en droit français prend d’ailleurs une longueur d’avance sur le texte européen en portant une attention particulière au phénomène des deepfakes[15].

En France, seuls les textes fictionnels décrivant des abus sexuels sur mineurs ou faisant l’apologie de la pédocriminalité échappent à l’interdiction.

## B – Qualifier un contenu terroriste

**Droit applicable.** En droit français, la notion de contenus terroristes en ligne, au sens de la LCEN, peut relever de deux infractions distinctes que sont le délit d’apologie du terrorisme et le délit de provocation à la commission d’actes terroristes. Ces interdictions résultent du libellé de l’article 421-2-5 du Code pénal :

> “Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l’apologie de ces actes est puni de cinq ans d’emprisonnement et de 75 000 € d’amende. Les peines sont portées à sept ans d’emprisonnement et à 100 000 € d’amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.”

**Absence de définition.** La loi s’abstient toutefois de définir les notions d’apologie et de provocation. Les contours de ces deux interdits ont donc été dessinés au fil des décisions de justice relatives à des actes de nature terroriste.

**Apologie.** En l’état actuel du droit, l’apologie publique est regardée comme l’expression d’une opinion qui présente un acte terroriste ou son auteur sous un jour favorable et à destination d’un groupe de personnes non déterminé[16]. Pour être constituée, l’apologie doit réunir un élément matériel, une incitation publique à juger positivement un terroriste ou un acte terroriste, et un élément moral, c’est-à-dire déceler l’intention de valoriser cet acte ou cet individu.

**Exemples.** En pratique, au-delà de la seule glorification, l’apologie recouvre également des propos ayant vocation à justifier de tels actes ou à défendre leurs auteurs. Ainsi, qualifier des personnalités terroristes de “courageux” constitue bien une apologie de ces derniers[17]. A l’inverse, l’évocation, même sur un ton menaçant, d’organisations terroristes ne suffit pas pour que le délit d’apologie soit constitué. À titre d’exemple, la Cour de cassation s’est refusée à qualifier d’apologie du terrorisme les intimidations et menaces opérées par un individu sur ses interlocuteurs, alors que celui-ci se revendiquait d’une mouvance terroriste. Son propos ayant au contraire vocation à générer chez eux de la crainte ou du rejet, cela empêchait de porter un regard favorable sur cette organisation[18].

15 Une définition légale du deepfake émergerait du projet de loi SREN (Sécuriser et Réguler l’Espace Numérique), en insérant à l’article 226-8 du Code pénal une mention incluant “un contenu visuel ou sonore généré par un traitement algorithmique et reproduisant l’image ou les paroles d’une personne, sans son consentement, s’il n’apparaît pas à l’évidence qu’il s’agit d’un contenu généré algorithmiquement ou s’il n’en est pas expressément fait mention”. Amendement déposé par le Gouvernement, adopté devant le Sénat français en juillet 2023.
16 Cass. crim. 7 janvier 2020, n°19-80.136
17 Cass. crim. 27 novembre 2018, n°17-83.602
18 Cass. crim. 4 juin 2019, n°18-85.042

**Provocation à la commission d'actes.** La provocation directe à la commission d'actes terroristes est une infraction elle aussi strictement encadrée. Contrairement à l'apologie, qui concerne des actes déjà commis ou leurs auteurs, la provocation incrimine le fait d'appeler à commettre des actes de nature terroriste. De nouveau, la jurisprudence est venue préciser ce concept, indiquant qu'il suppose la caractérisation d'une entreprise individuelle ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur[19]. Face à ce type d'infraction, il est indispensable de se livrer à une analyse contextuelle, ce qui permettra d'apprécier divers éléments tels que la cible, l'audience ou le cadre de la prise de parole.

**Diversité des contenus.** Au-delà de la provocation directe à la commission d'actes terroristes ou de l'apologie d'attentats déjà commis, il faut appréhender comme illicite tout contenu incitant à la commission d'actes terroristes, sollicitant un ou des individus pour commettre un acte terroriste ou participer à des activités d'un groupe terroriste, fournissant des instructions quant à la fabrication ou l'utilisation d'armes ou de substances dangereuses[20] ou constituant une menace quant à la commission d'actes terroristes[21].

**Vigilance.** La connaissance de ces critères précis est nécessaire afin de ne pas tomber dans l'écueil de la sur-modération face à ce type de contenus. Des contenus non-violents peuvent être illicites et inversement, des contenus potentiellement choquants peuvent être utilisés à des fins d'information, de recherche ou de militantisme. Il convient donc de différencier les publications visant à dénoncer la propagande terroriste, qui ne tombent pas sous le coup de la loi, et celles qui visent à en faire la promotion, assimilées à de l'incitation au terrorisme.

**Précaution.** La langue utilisée dans certaines publications peut parfois rendre complexe leur compréhension, et donc leur qualification juridique. Dans pareils cas, il est conseillé de signaler tout contenu portant un signe visuel distinctif qui le rattache directement à un groupe terroriste identifié, ou à l'un de ses médias. La mission des personnels chargés de ces contenus est d'évaluer leur licéité. Si cette appréciation peut paraître évidente dans de nombreux cas, certains contenus posent question. En cas de doute, il est conseillé de transférer les signalements aux autorités qui procéderont à une qualification juridique ou de faire appel, par exemple, à l'association professionnelle Point de Contact, plateforme associative dédiée au traitement des signalements de contenus illicites.

19 Cass. crim. 10 janvier 2023, n°20-85.968
20 Aussi réprimée par l'article 322-6-1 du Code pénal français.
21 Article 2, point 7 du Règlement (UE) relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *op.cit.*

# III – Le traitement des signalements

## A – Le transfert aux autorités

**Droit applicable.** La LCEN et le DSA n'imposent pas à l'hébergeur une obligation générale de surveillance des informations qu'il transmet ou stocke[22]. La deuxième obligation faite aux hébergeurs consiste cependant à informer promptement les autorités publiques compétentes dès lors qu'ils ont connaissance qu'un contenu ou qu'une activité illicite est hébergé sur leurs services.

### 1 – PHAROS[23] : la plateforme nationale de signalement des contenus illicites

**Présentation.** Pour pouvoir recevoir les signalements du grand public et des acteurs de l'Internet, les autorités ont mis en place une cellule dédiée. La plateforme PHAROS, composée de gendarmes et de policiers, a ainsi été mise en service le 1er septembre 2006 au sein de l'OCLCTIC[24] et centralise les signalements adressés aux autorités. Son rôle est d'analyser les infractions en ligne, les qualifier, et d'assurer, lorsque nécessaire, le traitement judiciaire des contenus illégaux.

**Dispositif de signalement.** Un formulaire en ligne[25] est mis à disposition du public, qui permet à toute personne de signaler tout type d'infraction rencontré lors de sa navigation en ligne. Des organismes privés peuvent signer une convention de partenariat avec la plateforme PHAROS afin de se voir attribuer un compte de signalant professionnel.

**Diversité des contenus.** Il est important de rappeler ici que PHAROS ne traite pas uniquement les délits sur lesquels se concentre ce livre blanc. PHAROS reçoit et traite également nombre d'autres types d'infractions commises en ligne.

**Diversité des infractions.** Pour les personnes travaillant en majorité sur des contenus contenant de la propagande terroriste, il est recommandé de leur permettre de distinguer de tels contenus des contenus relevant de "Menaces ou incitation à la violence ou d'Incitation à la haine"[26] notamment.

Pour ce qui est des professionnels en charge du traitement de contenus CSAM (Child Sexual Abuse Material), il est également utile qu'ils soient familiarisés avec la qualification de contenus autrement illicites, comme par exemple ceux relevant du trafic illicite, ou toute autre forme d'abus sexuels sur une personne mineure comme la manipulation psychologique d'un enfant à des fins sexuelles.

Enfin, une consultation de la base de données Lumen[27] peut être une aide précieuse pour tout employé souhaitant connaître les types de contenus géo-bloqués en France

22 Article 6-1-7 de la Loi n° 2004-575 pour la confiance dans l'économie numérique, *op.cit.* ; Article 8 du Règlement (UE) relatif à un marché unique des services numériques (DSA), *op. cit.*
23 Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements.
24 Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
25 https://www.internet-signalement.gouv.fr
26 Ce type d'infractions est notamment réprimé par l'article 24 de la loi sur la liberté de la presse, 29 juillet 1881.
27 https://www.lumendatabase.org/

sur le fondement de diverses dispositions légales.

**Formation des personnels.** Il est fortement conseillé de s'assurer que les personnes en charge du traitement des signalements illicites sont informées de la liste complète des motifs de signalements du formulaire PHAROS. Cela permet, d'une part, de s'assurer que les contenus sont envoyés vers les unités désignées afin d'en assurer un traitement rapide par des agents spécialisés et, d'autre part, cela élargit le champ de compétences des personnes en charge du signalement au-delà des seules infractions d'exploitation sexuelle de mineurs ou relatives à la propagande terroriste.

### 2 – Les suites données aux signalements

**Redirection pertinente.** PHAROS redirige les signalements vers les services de police ou de gendarmerie territorialement compétents, ou encore vers des services spécialisés, en fonction de la nature des contenus à traiter (C3N[28], OCRVP[29], etc.). Pour les affaires à dimension internationale, PHAROS se rapproche de l'agence INTERPOL.

**Qualité du signalement.** Les signalements n'ont pas valeur de plainte, mais de renseignement. Ils sont généralement exploités par PHAROS selon le schéma suivant :

- Vérification de l'existence du contenu signalé (est-il toujours en ligne ?) ;
- Qualification juridique (est-il illicite au regard de la loi française ?) ;
- Mesures conservatoires (sauvegarde des contenus et des éléments d'enquête, enrichissement et recoupement d'informations, vérifications techniques, investigations en source ouverte, intégration et comparaison d'images dans la base de données du CNAIP[30]), détermination du service destinataire (si nécessaire au moyen d'investigations complémentaires) ;
- Ouverture d'une enquête.

OU

- Transmission du signalement à un service de police ou de gendarmerie compétent ou à un service étranger via INTERPOL ;
- Ouverture d'une enquête par le service saisi ;
- Suivi du signalement (conseils au service destinataire et retour d'informations).

**Compétences administratives.** L'OCLCTIC, et en son sein PHAROS, est l'autorité administrative compétente pour émettre des injonctions de retrait à l'encontre de contenus à caractère terroriste et pédocriminels[31]. Quand le retrait du contenu ne peut pas être obtenu, elle dispose d'une compétence exclusive pour procéder au blocage administratif[32] des contenus pédocriminels et de propagande terroriste, permettant d'empêcher tout accès à ces contenus par l'intermédiaire des fournisseurs d'accès à

28 Centre de lutte contre les criminalités numériques du pôle judiciaire de la gendarmerie nationale
29 Office central pour la répression des violences aux personnes
30 Centre National d'Analyse d'Images Pédopornographiques, intégré au C3N
31 Article 1er du décret n° 2023-432 du 3 juin 2023 relatif au retrait des contenus à caractère terroriste en ligne
32 Article 1er du décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

Internet (FAI) français.

**Autorité de contrôle.** Ces procédures de retrait et blocage sont opérées sous la supervision de l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM)[33].

## B – Les actions et délais applicables

**Conservation des données.** Lorsqu'un contenu illicite est signalé à l'opérateur, celui-ci doit procéder, après qualification, à sa transmission aux autorités compétentes dans les meilleurs délais. Il doit ensuite le rendre inaccessible au public en ligne en veillant à laisser aux autorités la possibilité de procéder aux constatations nécessaires.

**Délai légal.** Le délai de conservation a été fixé par décret d'application de l'article 6-4 de la LCEN[34]. Il est fixé à six mois à compter de la date à laquelle le contenu en question a été retiré ou rendu inaccessible.

**Modalités.** Par-delà la durée de conservation, le décret impose que cette conservation soit assortie de garanties techniques et organisationnelles. Le caractère illicite de ces données, malgré ce devoir de conservation, rend leur manipulation particulièrement sensible. C'est pourquoi ces données doivent là aussi être isolées du reste des activités de l'hébergeur et accessibles par un personnel habilité. À cet égard, l'exploitation ou le traitement des données liées à ces contenus illicites ne peut avoir pour vocation que la lutte contre la cybercriminalité[35].

**Peines encourues.** Il convient donc de suspendre ou rendre inaccessible au public le contenu identifié, de ne surtout pas l'effacer, mais de le conserver et de l'isoler techniquement. La suppression de ces contenus et données associées est passible des sanctions prévues à l'article 434-4 du Code pénal[36]. L'hébergeur pourrait se voir reprocher d'avoir détruit des preuves et fait entrave à l'enquête.

**Modération interne.** Les conditions d'utilisation de ces services, établies par les plateformes et hébergeurs eux-mêmes, peuvent aussi jouer un rôle crucial en leur permettant d'agir malgré l'absence d'illicéité constatée pour prévenir de potentiels dommages. Les entreprises incluent bien souvent des dispositions spécifiques permettant des actions de modération lorsque la qualification légale des contenus est incertaine.

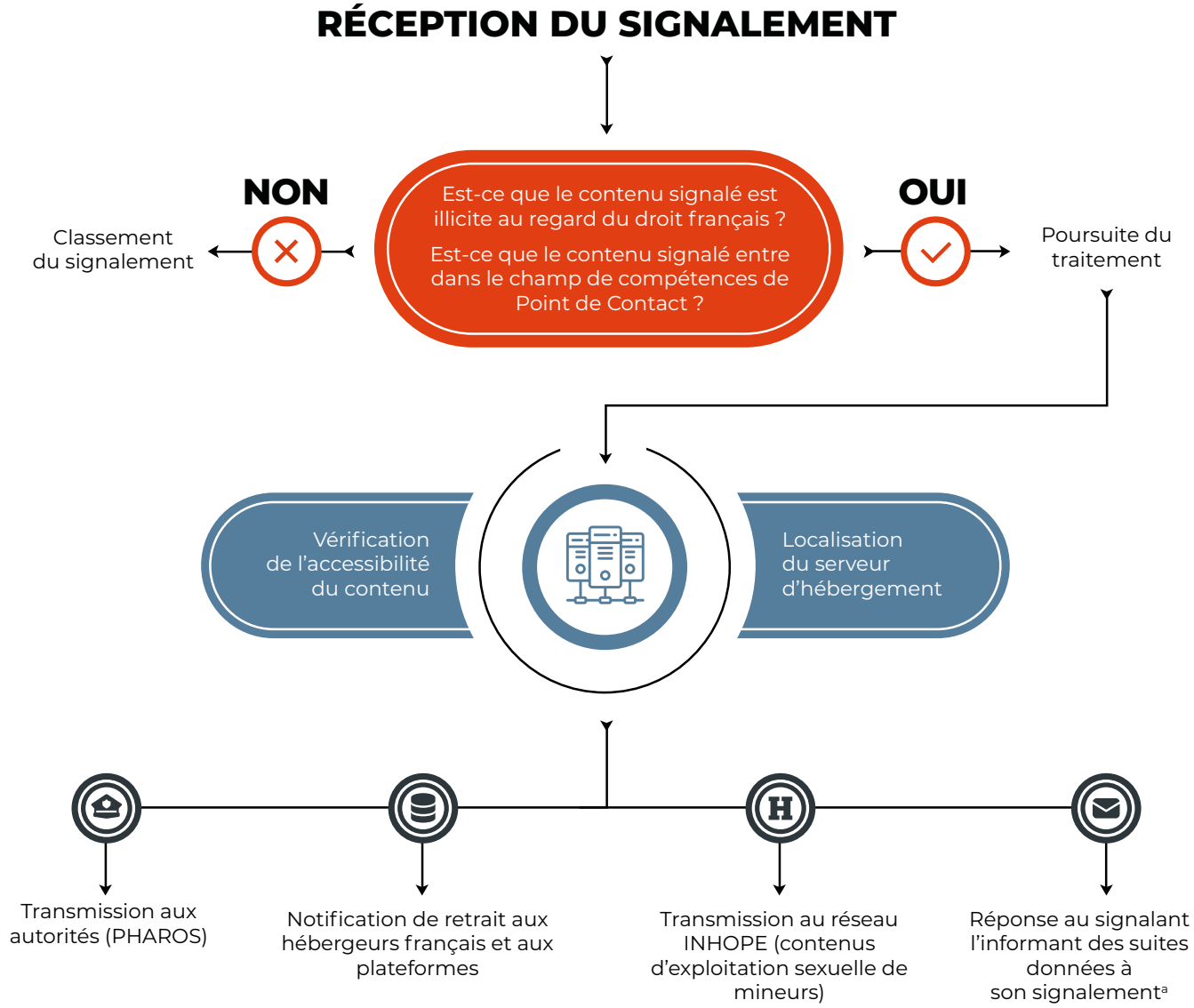
**Diversité des actions.** Chaque acteur peut ainsi établir des politiques internes de modération face à des contenus qu'il ne souhaite pas voir se diffuser sur ses services. La pratique a vu émerger une variété de dispositifs destinés à limiter l'impact de

33 Article 6 du décret n° 2023-432 du 3 juin 2023, op. cit et Article 3 du décret n° 2015-125 du 5 février 2015, op. cit.
34 Article 1er du décret n° 2022-1567 du 13 décembre 2022 relatif à la conservation des contenus retirés ou rendus inaccessibles par les opérateurs de plateforme en ligne soumis à des obligations renforcées en matière de lutte contre la diffusion publique de contenus illicites
35 Article 2 du décret n° 2022-1567 du 13 décembre 2022, op cit.
36 Article 434-4 du Code pénal

certains contenus ; rappel des règles à l'utilisateur ou avertissement, réduction de la visibilité, filtre protégeant la sensibilité de la communauté, démonétisation, etc.

**Vigilance éthique et légale.** Les actions entreprises par les plateformes et hébergeurs en l'absence de qualification d'un contenu illicite soulèvent alors nécessairement des questionnements éthiques. Il reste qu'il est essentiel que ces entreprises garantissent une prise de décision transparente et proportionnée à l'atteinte au droit fondamental à la libre expression que constitue ce type de décision de modération. Il est par ailleurs indispensable de mettre en place des mécanismes de recours pour les utilisateurs afin de contester les décisions de modération prises par les plateformes[37].

## Procédure de traitement des signalements par Point de Contact




37 Article 20 du Règlement (UE) relatif à un marché unique des services numériques (DSA), *op. cit.*

a Si nécessaire, Point de Contact peut également apporter des conseils aux signalants et les réorienter vers des structures adaptées.

# PARTIE II
# LA PROTECTION DES PROFESSIONNELS

**Dimension humaine.** La première partie de ce document a traité des méthodes et des processus opérationnels qu'une organisation peut mettre en place afin de recevoir, qualifier et signaler des contenus en ligne choquants et potentiellement illicites. Jusqu'ici, le document a traité de définitions légales, de processus de qualification, de formats de signalement... Autant de procédés techniques qui n'ont que très peu abordé un point essentiel : l'aspect humain de ce travail.

**Singularité.** Or, l'exposition à ces contenus choquants n'est pas une chose "normale" ou "habituelle" pour de nombreuses organisations. Les professionnels qui sont exposés à ces contenus l'étant dans le cadre de leur activité professionnelle, un cadre approprié doit être mis en place par l'employeur afin d'assurer que la santé et le bien-être de ces professionnels soient le moins impactés possibles par le travail en question.

**Déroulé argumentatif.** Ainsi, cette seconde partie du livre blanc traitera de ce qu'il conviendrait, pour les organisations, de mettre en place afin de protéger leurs professionnels. On définira d'abord ce que peut englober le terme de "professionnels exposés à des contenus choquants" (I), avant d'aborder ensuite l'aménagement des conditions de travail (II), l'encadrement psychologique destiné à protéger ces personnels (III), puis la prévention contre les risques psychosociaux (IV).

# I – Les professionnels exposés à des contenus choquants

**Devoir de protection.** L'une des principales missions de la lutte contre les contenus illicites consiste à assurer la protection du public. Cette préoccupation découle du fait qu'une simple exposition, ponctuelle ou unique, à des contenus violents peut engendrer des traumatismes.

**Élargissement du spectre.** Il est néanmoins primordial de reconnaître la complexité de la chaîne de métiers impliqués dans cette lutte, une diversité d'acteurs dont la portée échappe souvent à notre connaissance. Si l'intention est ici de mettre l'accent sur les personnels fréquemment confrontés à des contenus violents, cela peut aussi constituer une opportunité d'élargir les perspectives de réflexion à l'égard de secteurs non-numériques, souvent oubliés. Cela induit de considérer un vaste ensemble de professions qui est également confronté à des contenus choquants et/ou à des situations particulièrement stressantes.

**Démarche globale.** Dans cette optique, il est impératif de considérer l'ensemble des acteurs engagés dans la lutte contre la cybercriminalité, d'identifier leurs besoins particuliers en matière de soutien psychologique et de sensibilisation, et de mettre en place des mesures adéquates visant à préserver leur bien-être mental et émotionnel. Une telle démarche contribuerait à la sauvegarde de leur intégrité, dans un contexte où leur mission de protection du public est d'une importance prioritaire.

**Professions judiciaires.** Si les enquêteurs, par exemple, sont exposés à un risque majeur, leur formation plus approfondie et leur accès à un suivi psychologique adapté viennent partiellement compenser une certaine vulnérabilité inhérente à leur métier. En revanche, les juges judiciaires, les avocats, les interprètes et les greffiers sont actuellement dépourvus de tout accompagnement ou sensibilisation destinés à préserver leur bien-être mental dans l'exercice de leurs fonctions. En tant que tel, ces professions sont susceptibles de connaître une exposition comparable à celles issues du secteur numérique et pourraient à ce titre bénéficier d'une protection similaire.

**Professions administratives.** De manière analogue, le personnel administratif connaît également des contraintes et des taux d'exposition importants, de même que les juges administratifs, appelés à statuer sur les injonctions de retrait, ne bénéficient pas encore nécessairement de la formation appropriée. Il s'avère essentiel de leur accorder par ailleurs un accès à une prise en charge individuelle et/ou collective dispensée par des professionnels de santé formés à ces enjeux.

**Modération communautaire.** Les modèles de modération des plateformes sont divers et variés et reposent parfois sur la communauté d'utilisateurs elle-même. Dans ce type de situation, il convient de noter que les personnes impliquées sont des volontaires plutôt que des professionnels. Bien que toutes les pratiques susmentionnées ne leur soient pas nécessairement applicables, certaines d'entre elles pourraient néanmoins être adaptées à leur situation.

# II – L'aménagement des conditions de travail

## A – Considérations humaines et technologiques

### 1 - Ressources humaines

**Introduction.** De nombreuses considérations liées à des décisions émanant du département des ressources humaines peuvent être prises en compte lorsqu'une organisation met en place des opérations de modération de contenus. Par ailleurs, il est fondamental que la plateforme qui recourt à une modération externalisée veille à ce que le prestataire s'inscrive dans les bonnes pratiques professionnelles en la matière.

**Collaboration.** À ce titre, l'organisation du travail doit pouvoir s'effectuer en collaboration avec la médecine du travail. Cette dernière assurera d'une part le suivi médical renforcé de ces personnels exposés et d'autre part, par son action en milieu de travail, pourra repérer les difficultés et transmettre toutes les recommandations nécessaires pour réduire le risque pour la santé (horaires de travail, conditions de travail, orientation vers les réseaux de soins ou de soutien psychologique...)[38].

**Contrat de travail.** Des clauses spécifiques peuvent aborder des aspects tels que la nature sensible du contenu traité, les mesures de confidentialité et de sécurité requises, ainsi que les obligations légales et éthiques inhérentes à la profession. C'est l'occasion de préciser les conditions d'accès aux contenus sensibles, en spécifiant les restrictions concernant l'utilisation d'appareils personnels ou de réseaux autres que ceux fournis par l'employeur. En incluant ces clauses, les employeurs s'assurent que les professionnels comprennent pleinement leurs responsabilités et les mesures spécifiques qui doivent être prises pour préserver leur bien-être et garantir une approche professionnelle dans la réalisation de leurs missions.

**Locaux.** Le traitement de contenus choquants nécessite un aménagement spécifique de l'espace de travail. Les personnels qui ne sont pas habilités à traiter ces contenus, et toutes les personnes amenées à être présentes dans les locaux, ne doivent en aucun

38 Le Centre national de ressources et de résilience est un partenaire important de la médecine du travail et met à disposition des personnes impliquées divers modules destinés à informer et sensibiliser sur ces questions.

cas être susceptibles d'y accéder, de les visualiser ou de les entendre. Les locaux, ou espaces dédiés, devraient également être signalisés par un avertissement interdisant l'accès aux personnels non habilités.

Il convient de penser à protéger l'environnement extérieur de l'exposition aux contenus traités. Les fenêtres des locaux peuvent être assorties d'un dispositif opacifiant, si les espaces de travail sont susceptibles d'être vus de l'extérieur.

**Non-exclusion des personnels.** Néanmoins, et malgré les contraintes d'aménagement exposées ci-dessus, il faut veiller à ne pas isoler les professionnels de manière excessive afin qu'ils ne se sentent pas mis à l'écart de la vie de la structure qui les emploie. On pourra penser à mettre en place des opportunités pour que les équipes de modération puissent expliquer en interne en quoi consiste le travail de modération de contenus, afin de démystifier, éduquer les collègues, et trouver des aires de collaboration avec d'autres équipes de l'organisation.

**Gestion des personnels.** Le travail sur ce genre de contenu peut conduire à une sur-implication émotionnelle des employés. Les structures de gestion devront ainsi s'assurer d'une stricte déconnexion des personnels exposés en dehors de leurs heures de travail. Le recours aux heures supplémentaires et astreintes devra être particulièrement surveillé, pour garantir un temps de repos et de déconnexion suffisant des personnels concernés.

**Télétravail.** La tendance actuelle est au développement du télétravail[39], il est néanmoins très fortement déconseillé d'autoriser cette pratique lorsqu'il est question de procéder au traitement de contenus. Associer l'espace que constitue le domicile personnel à un environnement d'images violentes peut nuire au salarié et à son entourage familial – en cas d'exposition accidentelle par exemple. La consultation de ces contenus, pour partie illicites, doit être réservée au cadre strictement professionnel, car cette consultation est nécessairement dérogatoire. Cela suppose donc que l'accès à ceux-ci par le biais d'un appareil privé ou d'un autre réseau que celui mis à disposition par l'employeur soit rendu impossible.

**Exceptions.** Certaines dérogations peuvent être envisagées dans des situations particulières où le travail est effectué exclusivement à distance ou lorsque des circonstances exceptionnelles l'imposent.

Lors d'urgences ou de situations critiques où une intervention immédiate est requise, l'accès à distance peut être autorisé pour permettre une réaction rapide et efficace.

Autre exemple, dans le cas de services de modération fonctionnant 24 heures sur 24 et 7 jours sur 7. Il peut être nécessaire de permettre aux professionnels de télé-travailler afin d'assurer cette couverture continue, il sera alors recommandé que l'équipe se rencontre tous les jours afin que le manager puisse s'assurer du bien-être de son équipe.

Cependant, même dans ces situations, il est crucial de mettre en place des protocoles stricts pour garantir la sécurité et la confidentialité des données, ainsi que de fournir un soutien adéquat aux professionnels travaillant à distance.

39 Article L1222-9 du Code du travail régissant divers aspects du télétravail.

## 2 - Techniques et technologies

En plus de ces considérations “RH”, il pourra être mis en place un certain nombre de techniques et technologies afin d’assurer que seuls les personnels habilités sont exposés aux contenus choquants, et qu’eux-mêmes soient impactés le moins possible.

**Postes de travail.** Les ordinateurs utilisés aux fins d’analyse de contenus devraient être a minima protégés par des mots de passe complexes et non accessibles. En complément de cette sécurisation, il est recommandé de chiffrer ces machines. On pourra enfin réfléchir à la possibilité de créer un espace de stockage (en local ou en cloud) séparé du reste du stack technique (ensemble des outils technologiques) utilisé par l’organisation.

**Équipements.** Par ailleurs, il est conseillé d’assortir les écrans de filtres de confidentialité, ou de les orienter de manière à ne pas exposer le reste du personnel, ou l’extérieur.

Un casque audio est recommandé pour évaluer les bandes sons des vidéos, lorsque cela est nécessaire. Il est cependant à noter que la bande son assortie d’une vidéo peut accroître le risque traumatique du contenu consulté. La lecture de la bande son d’une vidéo ne devrait être réalisée que lorsqu’elle est indispensable à la qualification du contenu.

**Solutions techniques pour mieux contrôler l’exposition.** En complément de mesures visant à minimiser l’impact des contenus choquants sur le bien-être des analystes, on pourra étudier l’implémentation de solutions techniques qui permettent de diminuer la fréquence d’exposition des personnels, voire même d’éviter des instances d’exposition qui ne seraient pas absolument nécessaires.

### α) *Fonctions de hachage*

Le hachage est la création d’une “empreinte numérique unique” (appellée « hash ») à partir d’un fichier image ou vidéo. Une telle empreinte pourra être créée pour chaque contenu qualifié de pédocriminel ou de terroriste par l’organisation, et ajouté à une base de données interne. À l’avenir, chaque nouveau contenu qui arrive dans le système de modération des contenus pourra être haché également, comparé aux empreintes identifiées comme illicites par le passé, et automatiquement qualifié, sans demander à un analyste d’être exposé au contenu (si l’organisation le permet - autrement dit, si une revue manuelle n’est pas jugée nécessaire dans 100% des cas d’identification de contenus illicites). Cette approche permet de ne pas exposer inutilement des analystes à des contenus choquants déjà connus.

Il est également possible de se connecter à des systèmes de partage de hashs déjà connus mis à disposition par des organisations non-gouvernementales, telles que l’Internet Watch Foundation[40] britannique, le National Center for Missing and Exploited Children[41] américain, ou encore Thorn[42] ; ou bien d’utiliser des services proposés gratuitement par des entreprises privées (Microsoft PhotoDNA[43], Google CSAI Match[44]).

40 INTERNET WATCH FOUNDATION, Image Hash List, https://www.iwf.org.uk/our-technology/our-services/image-hash-list/
41 NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, CyberTipline 2022 Report, Hash Sharing, https://www.missingkids.org/cybertiplinedata#:~:text=Hash%20Sharing
42 THORN, Outil Safer, https://safer.io/how-it-works/
43 MICROSOFT, Outil PhotoDNA, https://www.microsoft.com/en-us/photodna
44 GOOGLE, Outil CSAI Match, https://protectingchildren.google/tools-for-partners/#learn-about-our-tools

### β) *Système de priorisation*

Lors de la réception de signalements à traiter, la solution la plus simple consiste à ajouter ces signalements à une unique file d'attente, et à les traiter dans l'ordre d'arrivée, quels que soient les contenus concernés. Cette approche présente néanmoins deux problèmes majeurs : pas de priorisation en fonction de la gravité (supposée ou réelle) des contenus, et absence de spécialisation des modérateurs (n'importe quel membre de l'équipe pourra être amené à traiter n'importe quel type de contenu signalé). On peut y remédier en tentant de prioriser et organiser les contenus en attente de modération.

En plus de permettre de plus rapidement identifier les contenus les plus graves/sérieux, cette seconde approche présente plusieurs avantages au niveau du bien-être des modérateurs, notamment en évitant d'exposer des personnes novices aux pires contenus, ou en permettant à chaque modérateur de mieux organiser sa journée de travail (en choisissant à quel moment traiter quel type de contenu).

Cette priorisation pourra s'effectuer en créant des files d'attente de contenus séparées, qui seront chacune potentiellement traitées par des modérateurs différents, qui pourront développer des compétences spécialisées dans une ou plusieurs typologies de contenus choquants. Ces files d'attente pourront être nourries manuellement (par exemple, on pourra créer un mécanisme de signalement qui permette au public d'indiquer une catégorie de contenu illicite ou choquant) ou automatiquement (en utilisant des solutions comme la vision par ordinateur, ou d'autres méthodes telles que l'intelligence artificielle).

## B – L'environnement de travail

Une attention particulière peut-être portée à l'environnement de travail des personnels exposés.

**Solitude contre-indiquée.** Le professionnel qui analyse les contenus ne devrait pas travailler seul dans un bureau. L'isolement peut accroître le stress lié à l'exposition aux contenus et la présence de collègues dans l'espace d'analyse participe à mettre en confiance l'individu exposé.

**Soutien des personnels.** Le salarié devrait également pouvoir échanger, en cas de besoin, avec son responsable ou toute personne habilitée au sein de l'entité. Il est conseillé de faire des réunions d'équipe régulières au cours desquelles les conditions de travail peuvent être réévaluées.

**Gestion du temps d'exposition.** Il devrait avoir la possibilité de faire une pause à tout moment lorsqu'il travaille sur la qualification et, ainsi, pouvoir prendre du recul face à un contenu qui a pu le choquer.

Il est recommandé d'aménager un espace de détente à l'extérieur de celui qui est consacré à l'analyse afin de pouvoir plus facilement s'extraire de l'environnement lié aux contenus. Certaines entités mettent à la disposition du personnel des consoles de

jeux vidéo, des jeux de société, un baby-foot, un téléviseur, des supports de lecture ou encore proposent des activités sportives et/ou culturelles.

## C – Formation et accompagnement

**Formation.** Actuellement, il n'existe aucune formation académique spécialisée permettant aux analystes d'apprendre les techniques d'investigations ou le cadre juridique dans lequel le travail sur ce type de contenus doit être opéré.

**Rencontres professionnelles.** Afin de compenser ce manque de formation, les professionnels sont amenés à se rencontrer régulièrement, notamment à l'initiative des associations professionnelles. Ces rencontres ou colloques sont des moments d'échange privilégiés entre confrères. Le partage de connaissance et la transmission de bonnes pratiques y est favorisé.

Ces échanges peuvent porter sur des considérations techniques (conseils méthodologiques, mise en place de canaux de communications sécurisés, présentation d'outils ou de techniques d'investigation), juridiques (articulations des législations, projets de réglementations, veille jurisprudentielle), ou opérationnelles (protection des professionnels, mise en relations avec des confrères, interactions entre les secteurs publics et privés à des fins de collaboration).

Les temps d'échange formel ou informel entre professionnels de l'analyse de contenus extrêmes contribuent à maintenir un niveau de sociabilité facilitant la lutte contre l'isolement professionnelle, telle qu'explicitée plus haut. Il convient donc de faciliter et d'encourager la participation des professionnels à ces rencontres.

# III – La psychologie au cœur du métier

**Diversité des risques.** La nature même de ces contenus implique une forte charge émotionnelle ou psychologique, qui peut avoir des répercussions durables sur la santé ou la vie personnelle des personnels qui y sont exposés. Il n'existe pas de règle absolue en matière de résilience psychologique. Malgré tout, les effets de ces métiers sur la santé psychologique sont souvent minimisés par les personnels exposés, par fierté, pudeur, manque d'attention à soi, par peur du jugement, ou manque de sensibilisation aux effets insidieux engendrés par le traitement de ces contenus choquants.

**Encadrement personnalisé.** Pour l'entreprise ou la puissance publique, il convient donc de ne pas faire de généralisation sur la capacité d'une personne à être confrontée à ces contenus en fonction de son âge, de son sexe ou de sa situation familiale. Pour tous

les individus, les risques encourus, tel que l'état de fatigue psychologique, sont réels et doivent être pris au sérieux, quels que soient la fréquence et le degré d'exposition. Il est également à noter que certains contenus peuvent être plus choquants pour certains individus de par leur histoire personnelle.

## A – L'entretien psychologique préalable à la mission

**Information du candidat.** Protéger les personnels, c'est d'abord s'assurer de leur capacité à supporter l'exposition à ces contenus. La fiche de poste et l'entretien d'embauche devraient mentionner explicitement l'exposition à des contenus violents et choquants pour permettre au candidat d'accepter ou non le poste en parfaite connaissance des risques d'exposition. Il est recommandé de faire passer un entretien psychologique à tout candidat ou salarié pressenti pour occuper un poste comportant une telle exposition, et de l'en informer en temps utile.

**Déroulé.** Cet entretien préalable à la mission doit être réalisé par un psychologue clinicien ou un psychologue du recrutement et doit rester confidentiel. Cet entretien devra conduire à aborder explicitement des sujets tels que la conscience de la difficulté du poste, l'expérience du candidat, ses motivations, sa curiosité et interroger son aptitude à adopter un attitude résiliente face à de telles expositions.

**Objectifs.** Le but de l'entretien est de mesurer la prise de conscience par le candidat des missions qui seront les siennes, et des conséquences qu'elles pourraient avoir sur son équilibre psychologique, et ainsi juger de ses capacités à travailler en présence prolongée d'images potentiellement traumatisantes. À l'issue de celui-ci, le candidat devra également avoir une meilleure conscience de ses ressources personnelles, ce qui lui permettra de se projeter plus efficacement et plus justement dans de telles missions.

**Valeur contraignante.** L'avis du psychologue ne lie pas le recruteur mais permet de l'orienter dans ses choix. Il convient également de tenir compte du fait qu'une analyse psychologique s'apprécie à un instant T et ne préjuge en rien des changements psychologiques qui pourront être observés lors des entretiens ultérieurs.

**Précisions.** Le transfert de poste en interne vers une mission aussi particulière devrait toujours être consenti par le travailleur, qui doit comprendre la portée et les risques de la fonction, et bien appréhender les recommandations pour se protéger.

## B – L'accompagnement psychologique au cours de la mission

**Soutien obligatoire.** Une fois la personne recrutée, il est vivement conseillé de mettre en place un accompagnement psychologique obligatoire que seul un psychologue

clinicien est en mesure de réaliser. Ces consultations devraient être prises en charge intégralement par l'entreprise. Le psychologue du travail spécialisé dans la prévention des risques psychosociaux pourra être associé à l'accompagnement du chef de service ou de structure dans la prise en compte des situations évoquées par les personnels à des fins de prévention. Tous les personnels, quelle que soit leur ancienneté, doivent pouvoir bénéficier du même accompagnement.

**Identification du psychologue compétent.** Pour mener à bien les entretiens de supervision, le clinicien sera idéalement formé à la prise en charge des victimes de traumatismes (ex: formation auprès de France Victime, DU de victimologie…) et aura une solide expérience en la matière. Une formation à certaines techniques de prise en charge telles que l'EMDR[45] ou l'ICV[46] serait un plus. Dans une perspective préventive, ce spécialiste devrait être également en capacité de sensibiliser les professionnels à la gestion du stress et ses conséquences.

**Périodicité.** La fréquence des entretiens psychologiques obligatoires devrait être supérieure à un entretien annuel. Alternativement à ce suivi obligatoire, le professionnel exposé doit avoir accès à une consultation lorsque le besoin s'en fait sentir, sans avoir à obtenir l'accord préalable de son employeur, ni à l'en informer. De manière générale, les besoins des personnes exposées peuvent varier dans le temps et nécessiter des retours d'expérience aussi bien à froid qu'à chaud, donc conduire à des entretiens en dehors du cycle habituel.

**Diversité des profils.** Demander un entretien psychologique en dehors du suivi obligatoire ne devrait jamais être considéré comme un aveu de faiblesse ou un indicateur d'incapacité. Au contraire, le professionnel qui sait identifier les moments où son équilibre peut être menacé, et qui prend l'initiative d'en prévenir le risque, est bien plus à même de poursuivre sa mission dans de bonnes conditions que celui qui prendrait le parti de ne pas faire état de ses difficultés. Idéalement, l'entretien avec un psychologue doit devenir un outil de travail de nature à lui permettre d'adapter sa posture professionnelle tout en se préservant.

**Confidentialité.** L'entretien doit être confidentiel afin de permettre un échange libre entre le salarié et l'entité en charge du soutien psychologique. Néanmoins, le psychologue chargé de ce soutien doit pouvoir alerter en cas de risque pour le professionnel et/ou pour la structure, tout en respectant la confidentialité des entretiens. A minima, le psychologue devrait pouvoir alerter la structure via la médecine du travail de la nécessité de revoir le processus de traitement et de porter attention à la santé psychologique des personnes exposées. Les psychologues chargés de l'accompagnement des personnels doivent veiller à prendre toutes les mesures pour assurer leur protection.

**Sensibilisation managériale.** Il peut arriver qu'un professionnel soit dans l'incapacité de se reconnaître dans le besoin d'un soutien psychologique ou qu'il ne prenne pas

45 Eye Movement Desensitization and Reprocessing, qui peut se traduire par l' "Intégration neuro-émotionnelle par les mouvements oculaires" et qui constitue une méthode thérapeutique.
46 Intégration du Cycle de Vie, procédé thérapeutique ayant émergé au début des années 2000.

suffisamment en compte les risques que son état peut lui faire encourir. Il peut être envisagé de sensibiliser les responsables hiérarchiques à la reconnaissance des signes de potentiels risques psychosociaux, éventuellement à l'aide de l'intervention d'un médecin du travail. Il paraît important de sensibiliser l'ensemble de l'environnement professionnel à être bienveillant et attentif à des changements de comportement, pouvant traduire une lassitude passagère, associée ou non à des difficultés personnelles.

**Entretiens de groupe.** Des entretiens collectifs peuvent aussi être d'une grande valeur pour améliorer le travail d'équipe et construire une réflexion collective. Régulièrement organisés, ce second type d'entretien présente également une valeur ajoutée. En effet, si certaines personnes ont une parole plus libérée dans un cadre intimiste, d'autres s'expriment plus aisément portés par le groupe. Ce type d'environnement permet à plusieurs égards de briser une forme d'isolement. Les entretiens collectifs peuvent intervenir à date fixée, mais aussi à l'issue de phases ou d'événements spécifiquement difficiles.

## C – L'entretien psychologique par-delà la mission

**Accumulation des chocs.** Lorsqu'un professionnel achève sa période de travail en présence de contenus extrêmes, les images et vidéos auxquelles il aura été exposé ne quitteront pas pour autant son esprit. Le professionnel peut avoir vécu des épisodes de fatigue psychologique plus ou moins importants qui, s'ils n'ont pas été pris en charge suffisamment rapidement, pourraient perdurer après la fin de sa mission. Des altérations plus ou moins profondes peuvent aussi avoir pris place au niveau des représentations et conceptions morales, philosophiques, spirituelles, ou politiques. Les microtraumatismes psychologiques subis par un collaborateur ont un effet cumulatif dont la portée ne s'arrête pas au terme de la mission, de l'emploi ou de la carrière. Il faut considérer comme de la responsabilité du manager et des services de ressources humaines la nécessité de ce rappel.

**Entretien de fin de mission.** Il est conseillé de faire un entretien psychologique au moment où l'analyste quitte sa fonction. Cet entretien devrait lui permettre de faire un bilan de son expérience professionnelle, d'évoquer ce qui a pu l'affecter dans les sphères professionnelle et privée, et de déceler les conséquences qu'elle aura eu sur lui. Le psychologue devrait pouvoir lui apporter des conseils pour pouvoir faire face à d'éventuelles difficultés, ou pour pouvoir répondre à certains questionnements, qui se poursuivront, ou feront surface, dans l'avenir.

**Prolongement du soutien.** Bien que l'entretien de fin de mission possède une importance symbolique car il marque un terme à la période d'exposition au contenu graphique, il est important que le psychologue puisse donner une opinion quant à un éventuel accompagnement prolongé de l'analyste. Il est même de plus en plus souvent recommandé que les analystes disposent d'un soutien psychologique au-delà de la mission pour une période de 3 à 6 mois.

# IV – La prévention contre les risques psychosociaux

**Introduction.** Les spécificités et la professionnalisation continue de ce corps de métier (Trust & Safety) invitent finalement à venir au soutien d'une reconnaissance des difficultés inhérentes à ce type d'emplois. L'exposition régulière aux risques précédemment mentionnés implique d'envisager le potentiel nocif de l'activité professionnelle.

**Démarche préventive.** L'ensemble des recommandations formulées jusqu'ici ont en effet eu vocation à couvrir le risque de survenance de dommages de nature psychologique, causés par le travail, chez le professionnel. Ces mesures préventives – en opposition à des mesures réparatrices – sont des mécanismes conçus pour éviter ce que la médecine spécialisée nomme aujourd'hui les risques psychosociaux. L'approche retenue est ainsi d'amoindrir le risque que la santé du travailleur ne se dégrade en raison de son travail. Ces mesures sont censées permettre à l'employeur de garantir la santé et la sécurité de ses employés et donc de remplir les obligations légales dont il est débiteur[47].

**Définition.** L'identification de la nature de ces risques et des moyens de les prendre en charge est un travail qui a déjà été engagé. Les avancées scientifiques en la matière sont en effet nombreuses, tant sur le terrain de la médecine que de la sociologie, que du droit. Les travaux produits en ce sens font le constat d'usures anormales de l'organisme du travailleur, imputables au caractère éprouvant de l'activité exercée ainsi qu'au caractère singulier de certaines réactions biologiques ou psychologiques. L'exposition aux contenus extrêmes est ainsi par nature susceptible de générer un mal-être plus ou moins important chez le professionnel. Aussi le traitement régulier de contenus pédocriminels ou terroristes peut notamment engendrer un sentiment d'impuissance, une vision altérée, plus cynique, de la nature humaine, une perturbation des cycles de sommeil ou une consommation abusive de substances psychoactives[48]. La gestion de ces réactions appelle bien souvent un travail psychologique supplémentaire de telle sorte que le professionnel se trouve au croisement de multiples pressions psychosociales.

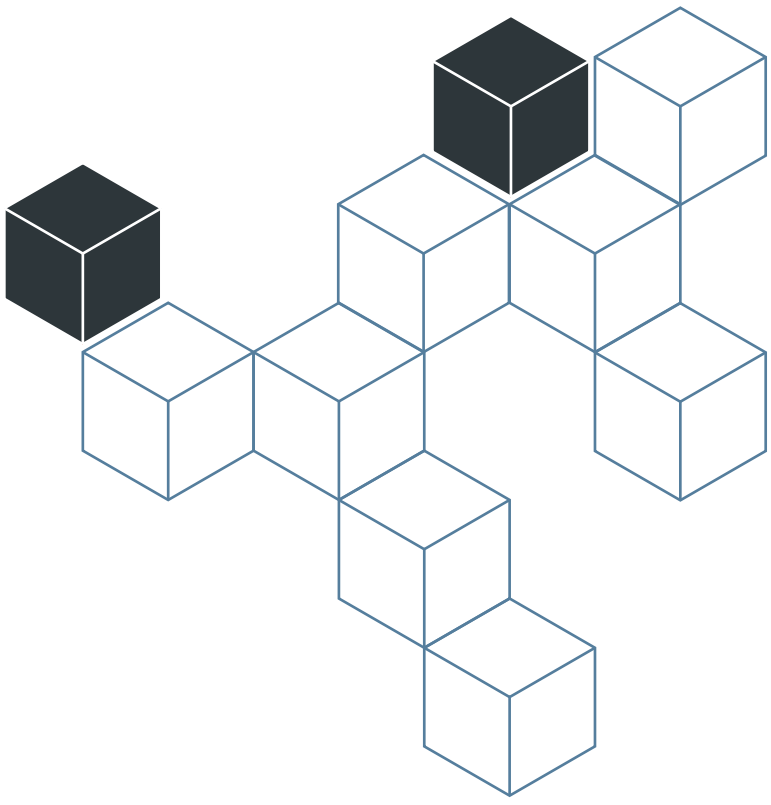
**Reconnaissance juridique progressive.** Bien que les réactions engendrées par l'exposition à ces risques varient d'un individu à l'autre, des éléments objectifs peuvent être utilisés à des fins de reconnaissance du risque professionnel. Il s'agirait dès lors de s'appuyer sur le caractère plus ou moins identifiable, durable ou supportable d'empreintes laissées par l'exposition à des contenus ou situations violentes ou choquantes sur l'organisme du travailleur. Cette approche a déjà reçu l'assentiment de certaines juridictions à travers le monde, lesquelles ont explicitement reconnu que le traitement de contenus extrêmes pouvait nuire à la santé des professionnels[49]. Un lien causal est alors établi entre le visionnage de violence graphique et la potentielle

47 Article L4121-1 et suivants du Code du travail.
48 Rae JEZERA, « Corporeal moderation : digital labour as affective good », Social Anthropology/Anthropologie Sociale (2021) 29, 4 928–943. © 2021 European Association of Social Anthropologists, doi:10.1111/1469-8676.13106, p.935-936.
49 Superior court of the state of California, Scola v. Facebook, 21 septembre 2018, civil action n°18CIV05135.

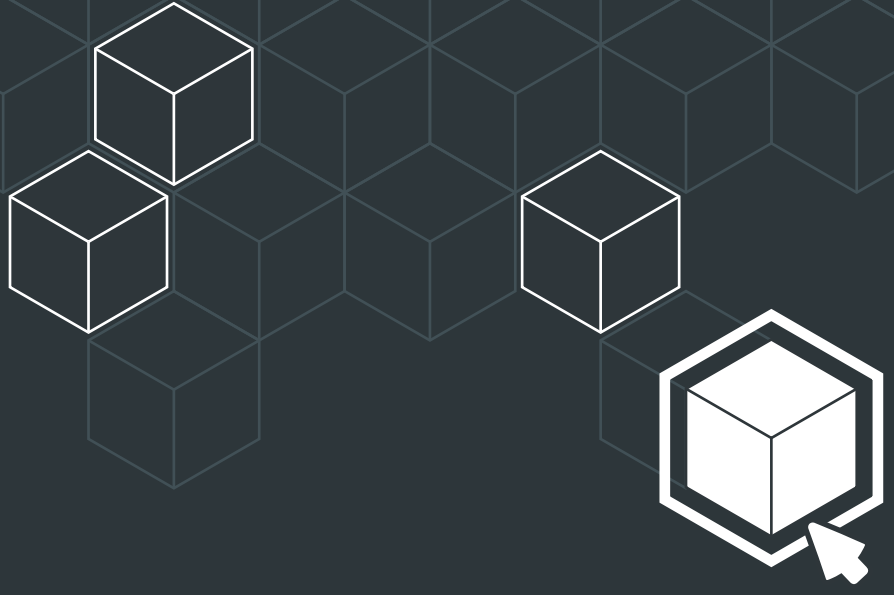
survenance de syndromes de stress post-traumatique[50], tout en admettant que ces symptômes puissent être différés dans le temps et survenir plus tard au cours de la vie[51]. Autrement dit, ce n'est pas parce que l'état de santé d'un professionnel paraît stable que les images visionnées n'ont pas eu d'impact sur son organisme.

À ce titre, un suivi est assuré en France par le biais du dossier médical en santé au travail et du document unique d'évaluation des risques professionnels (DUERP) au sein de l'entreprise. Ces derniers assurent la traçabilité des expositions à ces risques tout au long du parcours professionnel.

**Conclusion.** Par-delà les éléments pratiques évoqués plus haut, la logique commande également de penser théoriquement les finalités des efforts initiés dans le cadre de ce document de référence. Il s'agit de les inscrire dans une réflexion globale relative à l'utilité et l'effectivité des normes ainsi qu'à la lisibilité des dispositions légales. Les travaux ici engagés, en ce qu'ils prolongent le volet préventif des politiques relatives à la santé au travail, sont cruciaux. Il est néanmoins fondamental de ne pas regarder ce corpus de recommandations comme un unique recueil de bonnes pratiques mais aussi comme un vecteur de reconnaissance sociale, professionnelle et institutionnelle des risques auxquels sont exposés les professionnels confrontés à des contenus traumatisants.



50 Ibid. § 30
51 Ibid. § 35



# ANNEXES

# Le regard d'une psychologue spécialisée

## De la prévention du risque de traumatisme vicariant

Les contenus auxquels s'exposent les analystes sont violents et peuvent donc user. Ces professionnels sont donc un public à risque car la nature même du matériel traumatique à laquelle ils sont confrontés peut les conduire à vivre un traumatisme vicariant.

Le concept de traumatisme vicariant, ou traumatisme secondaire, a été proposé par deux psychologues, Laurie Pearlman et Karen Saatvine en 1995. Elles expliquent qu'un intervenant peut ressentir les mêmes séquelles par identification et compassion bien qu'il n'ait pas vécu le traumatisme directement.

Face à la répétition des séquences visuelles, « des images s'infiltrent, s'imposent, s'incrustent »[1][1]. Des changements profonds et durables de l'identité et la philosophie de vie apparaissent alors. « Le processus de traumatisation vicariante est [donc] une violation répétée de nos convictions, valeurs et croyances. » Il « touche directement l'identité, la vision du monde, la spiritualité. »[2] Le contexte de vie personnel actuel, l'histoire de vie et l'expérience professionnelle vont également avoir une incidence sur la propension à développer une symptomatologie traumatique.

**Heureusement, cette modification du cadre de référence personnel n'est pas inévitable.**

Il existe des stratégies personnelles d'autoprotection qui permettent à chacun de mettre à distance le matériel potentiellement traumatique tel que la capacité à prendre soin de soi, être empathique, être d'une nature optimiste[3]....

Un environnement de travail adéquat va également avoir un effet protecteur. Ainsi, des conditions de travail optimales prenant en compte la charge émotionnelle des salariés est à penser. Proposer un lieu de pause, d'échanges informels entre pairs est une vraie ressource.

Offrir un espace de parole via des réunions régulières, la mise en place de supervisions cliniques ou encore proposer des formations/sensibilisations sur la question du trauma permettra la mise en mots des maux.

Enfin, la prise en charge et l'orientation des personnels qui seraient impactés permettra de bonnes conditions de retour à l'emploi.

**Maïthé DUFÉTELLE**
Psychologue clinicienne
N° Adeli 949314231

1 *Les enseignants victimes de la violence*, Horenstein & Voyron Lemaire, collection MGEN, 1996.
2 Colloque *Les victimes d'actes criminels : agir dans le respect de la personne*, Christine Perreault, psychologue exerçant pour les services correctionnels au Canada, octobre 2004.
3 *Traumatisme Vicariant quand la compassion use*, Dossier Prévention au travail, été 2007.

# Le regard d'un philosophe spécialisé

## Être analyste, une profession de ... foi ?

**Réflexions philosophiques pour une éthique à venir.**

Dans n'importe quel domaine, le professionnel se distingue généralement de l'amateur en cela qu'il utilise, voire, crée des règles de métiers qui sont alors partagées pour accomplir du « bon travail » ou du « beau travail ». Il fait donc partie d'une communauté qui partage des pratiques, des manières de travailler, de résoudre des problèmes. Mais ce n'est pas tout.

Le mot « profession » a une origine religieuse que l'on a tendance à sous-estimer. Il désigne la manière dont, au Moyen-Âge, on parlait des chrétiens ou athées qui professaient leur foi en place publique. Professer sa foi, cela signifie essentiellement affirmer son appartenance à telle ou telle doctrine. Si bien que l'on pourrait dire qu'un professionnel est quelqu'un qui montre à tous les autres le fond de ses croyances théoriques à travers les pratiques concrètes de son métier.

Le problème de l'analyste qui s'expose, par et dans son travail, à toute sortes de violences et d'atrocités objectives, est pris dans l'évidence de lutter contre « le Mal » et d'être positionné dans le camp « du Bien », qu'il le veuille ou non, que ce soit dans la formation progressive de sa perception ou bien dans ce que lui renvoie ses proches ou ses collègues.

Il y a néanmoins un problème à croire que l'on est dans « Le Bien », avec des majuscules à l'expression – soulignons-le- car cela peut entraîner deux excès dans le comportement d'un analyste.

Le premier excès se caractérise par le phénomène du « Chevalier Blanc », à l'instar de Lancelot du Lac, dans Kaamelott, qui, comme on sait – même s'il était le plus « moral » et bien intentionné de tous les chevaliers - finit par devenir le Tyran de l'île de Bretagne. Au départ, il veut entraîner les autres vers la Lumière. Dans le phénomène du Chevalier Blanc, on trouvera des phénomènes désormais bien connus comme celui du « Sauveteur » ou bien celui du « Militant ». L'analyste a parfois l'impression de lutter dans l'ombre – caché de tous – pour des sujets plus qu'obscurs (les caniveaux les plus bas que l'on puisse imaginer concernant l'humain). Il est donc le Chevalier Noir aussi, autre versant du Chevalier Blanc.

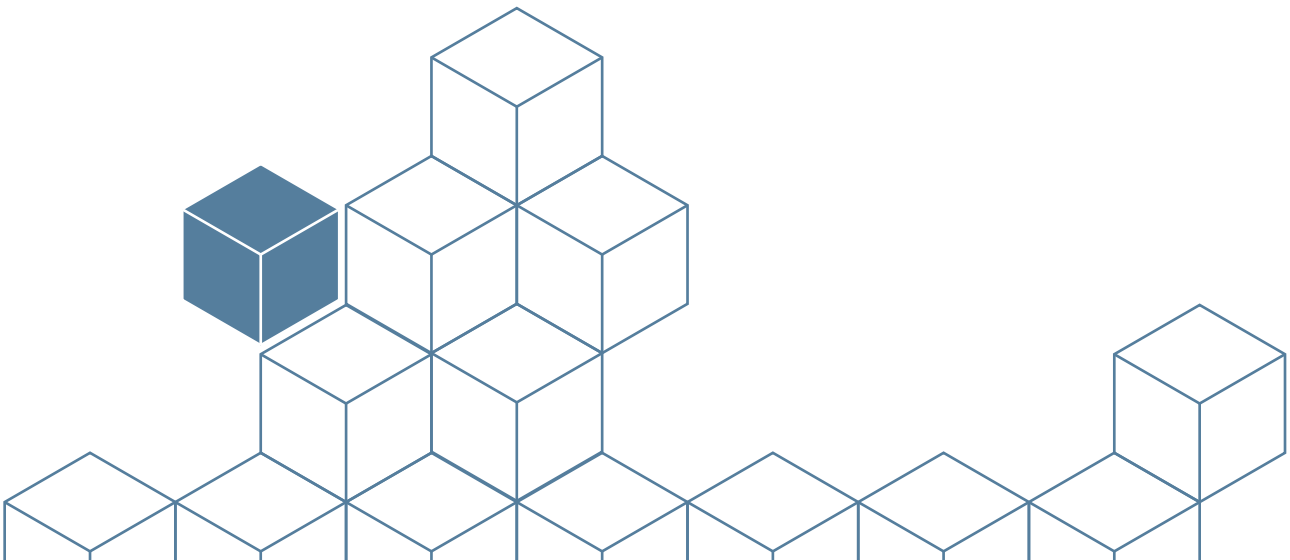
Le deuxième excès s'éprouve au travers de la dépression voire la mélancolie dans lesquelles on tombera facilement à considérer notre irréductible impuissance : impuissance à ne pas pouvoir enrayer « tout » le mal, impuissance devant la myriade de contenus existants, impuissance devant les réseaux qui semblent protéger les indignités, etc.

La morale est essentielle pour le vivre-ensemble. Ce qui nous apparaît comme « Mal » et « Bon » sont des boussoles tout à fait essentielles pour nous orienter dans la vie comme dans un métier. Il est difficile, dans une société où l'on a déconstruit ces notions

pour une prétendue « libération » des mœurs, de croire encore en de telles notions. Gageons qu'à la vue des contenus sexuels sur les mineurs notamment, l'évidence de cette polarisation entre le « Bien » et le « Mal » reste une évidence pour tous. Pour autant, il faut prendre le temps de penser l'autre polarité de nos mœurs que nous appelons la vie « éthique » qui se distingue et nous aide à penser la morale. Un professionnel a une « éthique », quand il connaît et partage une certaine manière de travailler qui définit ce que c'est que faire du « bon » et « beau » travail.

Car à n'être uniquement que dans la « morale », on devient soit moralisateur, soit démoralisé. Il est donc urgent de penser une éthique de la profession, c'est à cette condition – nécessaire mais non suffisante- que l'on pourra panser le métier d'analyste. À être un remède pour la société, il serait dommageable et scandaleux qu'il devienne un poison pour lui-même.

**Jean MATHY**
Philosophe et consultant, Directeur de Noetic Bees



# Liste des abréviations

| | |
|---|---|
| **ARCOM** | Autorité de Régulation de la Communication Audiovisuelle et Numérique |
| **CNAIP** | Centre National d'Analyse d'Images Pédopornographiques |
| **CSAM** | Child Sexual Abuse Material |
| **C3N** | Centre de lutte contre les criminalités numériques du pôle judiciaire de la gendarmerie nationale |
| **DSA** | Digital Services Act |
| **FAI** | Fournisseur d'accès internet |
| **LCEN** | Loi pour la confiance dans l'économie numérique |
| **OCLCTIC** | Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication |
| **OCRVP** | Office central pour la répression des violences aux personnes |
| **PHAROS** | Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements |
| **RH** | Ressources humaines |
| **RSN** | Règlement sur les services numériques* |

* Appellation française du DSA

# Bibliographie

## Législation


◇ Convention sur la cybercriminalité, Conseil de l'Europe, 2001

◇ Convention sur la protection des enfants contre l'exploitation et les abus sexuels, Conseil de l'Europe, 2007, dite "Convention de Lazarote"

◇ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE

◇ Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne

◇ Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie

◇ Loi du 29 juillet 1881 sur la liberté de la presse

◇ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

◇ Code pénal français :

- › Article 226-8
- › Article 227-23
- › Article 322-6-1
- › Article 421-2-5
- › Article 434-4

◇ Code du travail français

- › Article L4121-1 et suivants
- › Article L1222-9

◇ Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

◇ Décret n° 2022-1567 du 13 décembre 2022 relatif à la conservation des contenus retirés ou rendus inaccessibles par les opérateurs de plateforme en ligne soumis à des obligations renforcées en matière de lutte contre la diffusion publique de contenus illicites

◇ Décret n° 2023-432 du 3 juin 2023 relatif au retrait des contenus à caractère terroriste en ligne

# Décisions de justice

◇ Cour de Cassation, chambre criminelle, 10 janvier 2023, n°20-85.968

◇ Cour de Cassation, chambre criminelle, 7 janvier 2020, n°19-80.136

◇ Cour de Cassation, chambre criminelle, 4 juin 2019, n°18-85.042

◇ Cour de Cassation, chambre criminelle, 27 novembre 2018, n°17-83.602

◇ Superior court of the state of California, Scola v. Facebook, 21 septembre 2018, civil action n°18CIV05135.

# Colloques et conférences

◇ Colloque « Mieux protéger ceux et celles qui nous protègent », organisé par Point de Contact, 7 juin 2023, Sénat (Paris, France).

◇ Colloque « Organisation du travail et risques psychosociaux », organisé par l'Institut national de recherche et de sécurité pour la prévention des accidents du travail et des maladies professionnelles (INRS), 27 juin 2023, Maison de la RATP (Paris, France).

◇ Table-ronde "Time to care about Trust & Safety professionals", organisée par le Trust & Safety Forum, 5 avril 2023, Forum International de la Cybersécurité (FIC) (Lille, France).

# Thèses et ouvrages

◇ Placide ABASABANYE, « Analyse et mesure de la pénibilité au travail en France », Economies et finances, Université de Lille, 2021, français. NNT: 2021LILUA006. Tel-03366733

◇ Giorgia MACILOTTI, « La pédophilie et la pédopornographie en ligne, étude socio-criminologique des réalités italienne et française », 2012, Lille thèses

◇ Sarah T. ROBERTS, « Derrière les écrans. Les nettoyeurs du Web à l'ombre des réseaux sociaux », La Découverte, 2020, Chapitre 6.

# Études et rapports

◇ "Child Sexual Abuse Material, Model Legislation and Global Review", International Centre For Missing and Exploited Children (ICMEC), 9ème edition, 2018

◇ « Mesurer les facteurs psychosociaux de risque au travail pour les maîtriser », Rapport du Collège d'expertise sur le suivi des risques psychosociaux au travail, faisant suite à la demande du Ministre du travail, de l'emploi et de la santé, 2011

◇ THIEL, D., STROEBEL, M., and PORTNOFF, R. (2023). Generative ML and CSAM: Implications and Mitigations. Stanford Digital Repository. Available at https://doi.org/10.25740/jv206yg3793

# Revues et articles

◇ Rae JEZERA, “Corporeal moderation : digital labour as affective good”, Social Anthropology/Anthropologie Sociale (2021) 29, 4 928–943. © 2021 European Association of Social Anthropologists, doi:10.1111/1469-8676.13106

◇ Giorgia MACILOTTI, « Lutter contre la pédopornographie et le leurre d’enfants en ligne: la réponse policière française entre centralisme, dualisme et spécialisation », 2021

◇ Les Cahiers des RPS, « Travail et santé des organisations. Prévenir ensemble les risques psychosociaux. », Ministère du travail, revue biannuelle, n°31, juin 2018

# Guides

◇ « Guide de terminologie pour la protection des enfants contre l’exploitation et l’abus sexuels », Groupe de Travail Interinstitutionnel sur l’exploitation sexuelle des enfants, janvier 2016, ECPAT International et ECPAT Luxembourg, Mars 2017

◇ “M3AAWG Disposition of Child Sexual Abuse Materials Best Common Practices”, Messaging Malware Mobile Anti-Abuse Working Group, février 2015

◇ The Tech Coalition Industry Classification System. 2022. The Technology Coalition, July

◇ Building Resilient teams, Trust & Safety Professional Association

# Sitographie

◇ GOOGLE, Outil CSAI Match, https://protectingchildren.google/tools-for-partners/#learn-about-our-tools

◇ INHOPE – Réseau international de points de signalement , What is Child Sexual Abuse Material?, https://www.inhope.org/EN/articles/child-sexual-abuse-material

◇ INTERNET WATCH FOUNDATION (IWF) :

› Our MOU, the law and assessing content : https://www.iwf.org.uk/about-us/how-we-assess-and-remove-content/our-mou-the-law-and-assessing-content/

› Image Hash List : https://www.iwf.org.uk/our-technology/our-services/image-hash-list/

◇ INTERPOL, Pédocriminalité, https://www.interpol.int/fr/Infractions/Pedocriminalite

◇ MICROSOFT, Outil PhotoDNA, https://www.microsoft.com/en-us/photodna

◇ NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, CyberTipline 2022 Report, Hash Sharing, https://www.missingkids.org/cybertiplinedata#:~:text=Hash%20Sharing

◇ THORN, Outil Safer, https://safer.io/how-it-works/

# Table des matières

# Comité de rédaction

## Pilotage

**Vincent COURSON**
Partenariats Trust & Safety, Google

**Yann LESCOP**
Juriste - Analyste, Point de Contact

**Christian AGHROUM**
Commissaire divisionnaire honoraire, ancien chef de l'OCLCTIC, Membre honoraire de Point de Contact

**Quentin AOUSTIN**
Directeur des opérations, Point de Contact

**Flore BOUHEY-DWAN**
Experte Trust & Safety

**Julien CAUMOND**
Chef du Département atteintes aux personnes, Centre de lutte Contre les Criminalités Numériques (C3N), Commandement de la Gendarmerie dans le Cyberespace.

**Imen C-T**
Experte Trust & Safety

**Alexandre DANGREAU**
Head of Trust & Safety, OVHcloud

**Maïthé DUFETELLE**
Psychologue clinicienne

**Alain DOUSTALET**
Ancien responsable anti-abus chez Orange, Membre honoraire de Point de Contact

**Agnes EVRARD**
Directrice Trust & Safety, Brainly

**Florence FOULLON**
Médecin du travail, coordonnateur national du ministère de l'Intérieur et des Outre-Mer

**Nicolas HERNANDEZ**
Président, Aleph Networks, Trésorier de Point de Contact.

**Alexandre HUGLA**
Expert Trust & Safety, Gandi

**Jean-Christophe LE TOQUIN**
Président, Point de Contact

**Mick MORAN**
Enseignant au University College Dublin, ancien chef de l'équipe des crimes contre les enfants d'INTERPOL, Membre honoraire de Point de Contact

**Anne SOUVIRA**
Commissaire divisionnaire honoraire, ancien chef de la mission cyber de la préfecture de Police, Membre honoraire de Point de Contact

**Elisabeth ROLIN**
Présidente du corps des tribunaux administratifs et cours administratives d'appel, en service détaché