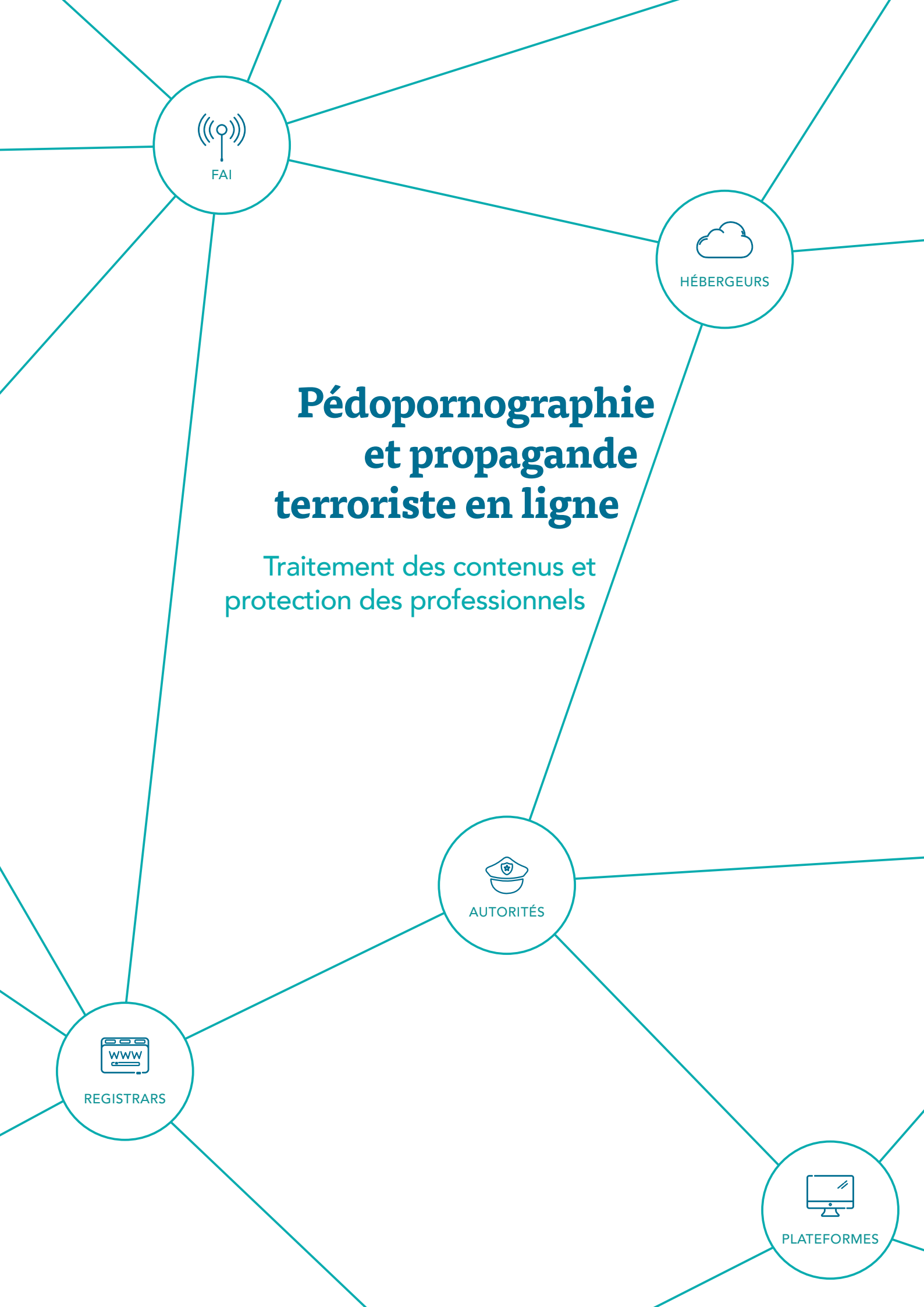


Pédopornographie et propagande terroriste en ligne

Traitement des contenus et protection des professionnels

TABLE DES MATIÈRES

INTRODUCTION – OBJECTIFS ET ENJEUX

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 la sécurité physique et l'équilibre psychologique des professionnels.

Les contenus choquants visés ici relèvent de deux catégories distinctes : les images ou représentations de mineurs présentant un caractère pornographique (art. 227-23 Code pénal), et les contenus de provocation à la commission d'actes terroristes et d'apologie du terrorisme (art. 421-2-5 Code pénal).

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

Le nombre des personnes en charge de traiter ces contenus a, par conséquent, fortement augmenté ces dernières années à travers le monde, et se compte aujourd'hui en milliers. Les petites entreprises, autant que les grandes, se voient de plus en plus contraintes de se doter de services consacrés à cette activité. Même si la technologie et l'intelligence artificielle permettent de renforcer considérablement l'efficacité de ces professionnels, la complexité de la qualification et l'enjeu de protection des personnes maintiennent la nécessité d'une intervention humaine.

Ce manuel s'adresse aux entreprises qui interviennent dans la diffusion de ces contenus : hébergeurs, plateformes de contenus, réseaux sociaux, registrars, fournisseurs d'accès à internet, autorités (services de police et de gendarmerie), ainsi qu'à toutes les personnes dont la responsabilité est d'intervenir, dans le cadre de leur activité professionnelle, sur ces contenus relevant d'activités cybercriminelles.

La protection des victimes qui apparaissent dans ces contenus, ainsi que la protection des personnes qui peuvent en être la cible, 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 tous les professionnels qui y sont confrontés, qu'ils y soient exposés régulièrement ou ponctuellement. Parce que ces personnels constituent une première ligne de défense essentielle, ce livre blanc entend contribuer à reconnaître leur rôle et la nécessité de prendre des mesures permettant d'assurer leur protection.

I) LA RÉCEPTION DES SIGNALEMENTS

La loi pour la confiance dans l'économie numérique (LCEN)[1] dispose que tous les hébergeurs, personnes physiques ou morales, doivent concourir à la lutte contre les contenus de provocation à la commission d'actes de terrorisme et leur apologie, ainsi que les contenus pédopornographiques[2], entre autres types de publications illicites.

L'obligation positive principale qui leur est faite se trouve à l'article 6-I alinéa 7 :

« […] À ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées […] »

A) Le dispositif de signalement

a) Mise en place d'un moyen de signalement

La première obligation est celle de mettre à disposition du public un moyen de signalement accessible et dont la procédure devrait pouvoir être intégralement poursuivie en ligne en quelques clics. Pour ce faire, il convient de mettre en place un dispositif dédié, simple, facilement identifiable et gratuit. Les contenus accessibles publiquement doivent pouvoir être signalés sans création de compte préalable. Il est en outre recommandé de proposer aux internautes la possibilité d'effectuer un signalement anonymement.

Un dispositif de signalement se matérialise le plus souvent par une adresse mail de type abuse@exemple.tld, ou par un formulaire dédié. Pour les contenus

---

1 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164

2 L'utilisation des termes « pornographie enfantine » et « pédopornographie » est de plus en plus critiquée en ce qu'ils associent l'enfant à la pornographie, qui ne devrait renvoyer qu'aux activités sexuelles entre adultes consentants, au lieu de souligner le statut de victimes d'exploitation et d'abus sexuels des enfants. Les termes « contenu d'abus sexuels sur mineur » apparaissent, entre autres, comme étant plus adaptés dans la mesure où ils soulignent le fait que l'enfant est victime, et non pas un acteur consentant et responsable de ses actes. Néanmoins, ce document conserve les termes « pédopornographie » et « contenus pédopornographiques » car ils sont utilisés par la législation française et européenne la plus récente et sont les plus connus du grand public. Pour plus d'information au sujet de la terminologie, voir les ressources documentaires en annexe du présent document.

édités sur les plateformes, l'internaute devrait pouvoir les signaler à tout moment lors de sa navigation sur la plateforme.

Il est recommandé de réserver le canal de signalement 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.)

b) Personnel habilité à la réception de signalement

La réception des signalements de contenus potentiellement illicites doit être réservée aux membres du personnel habilités à les traiter. 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/des salarié(s), et ne doit en aucun cas être imposé arbitrairement.

B) La qualification des contenus

a) Qualifier un contenu pédopornographique

Les contenus pédopornographiques et leur mise en ligne[3] sont visés par l'article 227-23 du Code pénal. L'alinéa 1 dispose que :

« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation. »

L'alinéa 1 précise que sont visés les contenus mettant en scène des mineurs, c'est-à-dire des personnes de moins de 18 ans. Si la détermination de la minorité ne pose généralement pas de difficultés, la distinction entre une personne mineure et une personne adulte n'est pas toujours évidente, surtout pour les adolescents[4].

La législation française vise indistinctement les contenus réels ou virtuels (ex. : dessins, photomontages ou trucages photographiques). En France, seuls les textes fictionnels décrivant des abus sexuels sur mineurs ou faisant l'apologie de la pédophilie échappent à l'interdiction.

Le contenu doit avoir un caractère sexuel. Cela exclut 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,

---

3 Art 227-23 al.3 : *« Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques ».*

4 Pour plus d'information, l'Évaluation de Maturité Sexuelle [nom original en anglais : Sexual Maturity Ratings (SMRs)] propose une classification des différents stades du développement pubertaire.

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

Le dernier alinéa de l'article 227-23 apporte une précision :

« Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. »

Il prévoit 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 conseillé d'effectuer un signalement.**

La loi française n'offre pas de définition précise de ce qu'est une image ou une représentation d'un mineur ayant « un caractère pornographique », mais d'autres sources[5] peuvent apporter un éclairage à cette question.

La directive 2011/93/UE[6] du Parlement européen et du Conseil du 13 décembre 2011 énonce dans ses définitions à l'article 2 :

« […] c) « pédopornographie » :

i) tout matériel représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ;

ii) toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles ;

iii) tout matériel représentant de manière visuelle une personne qui paraît être un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'une personne qui paraît être un enfant, à des fins principalement sexuelles ; ou

iv) des images réalistes d'un enfant se livrant à un comportement sexuellement explicite ou des images réalistes des organes sexuels d'un enfant à des fins principalement sexuelles ; […] »

5 Plusieurs sources, référencées en annexe, offrent des définitions d'un contenu à caractère pédopornographique.

6 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32011L0093&from=EN

b) Qualifier un contenu de propagande terroriste

Les deux premiers alinéas de l'article 421-2-5 du Code pénal nous donnent le cadre juridique de l'infraction :

« 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. »

Comment appréhender ce qui relève ou non de la provocation au terrorisme ou de l'apologie du terrorisme ? Le site officiel de l'administration française apporte un éclairage dans une fiche pratique consacrée à cette infraction[7] :

« Apologie du terrorisme

L'apologie du terrorisme consiste à présenter ou commenter favorablement des actes terroristes déjà commis. Par exemple, si une personne approuve un attentat.

L'apologie se distingue de la négation. La négation d'actes terroristes est lorsqu'une personne nie totalement ou partiellement ces actes sans les approuver directement. Si elle invoque un complot par exemple.

Pour être punie, l'apologie doit avoir été faite publiquement. Le caractère public des propos s'apprécie de la même manière que pour l'injure ou la diffamation. Ainsi, des propos tenus sur un réseau social ouvert au public peuvent être réprimés.

Provocation au terrorisme

La provocation au terrorisme est une incitation directe à commettre des actes terroristes matériellement déterminés. Par exemple, viser tel lieu ou telle personnalité. Par le contexte, la volonté de leur auteur et les termes choisis, de tels propos visent à convaincre d'autres personnes de commettre de tels actes.

Il s'agit d'une incitation à commettre des actes dans le futur et non d'une approbation d'actes déjà commis.

Il n'est pas nécessaire que de tels propos aient été tenus devant un large public. Des propos lisibles par quelques amis sur un réseau social ou prononcés lors d'une réunion privée peuvent être réprimés. »

7 https://www.service-public.fr/particuliers/vosdroits/F32512

Les contenus de propagande terroriste ne comportant pas d'images choquantes peuvent être illicites. **Le contexte a une incidence sur la qualification.** Chercheurs et journalistes peuvent utiliser ce type de contenus pour illustrer les résultats de leurs enquêtes. 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 ou à de l'apologie du terrorisme.

Par ailleurs, certains contenus choquants montrant des exactions violentes, et ne relevant pas de la provocation ou de l'apologie du terrorisme, peuvent malgré tout être illicites, en constituant, par exemple, une atteinte à la dignité de la personne humaine.

Au-delà de la provocation directe à la commission d'actes terroristes ou de l'apologie d'attentats déjà commis, il faut appréhender comme illicites les contenus qui tendent à faire adopter l'idéologie portée par un groupe terroriste, qui enjoignent à le rejoindre, ainsi que tout type de publicité ayant pour but d'en faire la promotion.

La langue utilisée dans certaines publications peut parfois rendre complexe leur compréhension, et donc leur qualification juridique. En pareil 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.**

II) LE TRAITEMENT DES SIGNALEMENTS

La mission des professionnels en charge de ces contenus est d'évaluer leur caractère manifestement illicite au regard de la loi française. 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[8], plateforme du secteur privé dédiée au traitement des signalements de contenus illicites.

A) Le transfert aux autorités

a) PHAROS[9] : la plateforme nationale de signalement des contenus illicites sur Internet

La deuxième obligation faite aux hébergeurs consiste à informer promptement les autorités dès lors qu'ils ont connaissance d'un contenu manifestement illicite hébergé sur leurs services. La LCEN n'impose pas à l'hébergeur une obligation générale de surveillance des informations qu'il transmet ou stocke[10] mais, dès l'instant où ce dernier a été informé de la présence d'une publication manifestement illégale sur son réseau, il doit en informer promptement les autorités compétentes.

Pour pouvoir recevoir à leur tour les signalements du grand public et des acteurs de l'Internet, les autorités ont mis en place une cellule dédiée. Ainsi, la plateforme PHAROS, composée de gendarmes et de policiers, a été mise en service le 1er septembre 2006 au sein de l'OCLCTIC[11] afin d'assurer le traitement judiciaire des signalements.

Un formulaire en ligne[12] a été 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.

---

8 Point de Contact est la plateforme française de signalement et de lutte contre les contenus illicites en ligne, https://www.pointdecontact.net/

9 Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements

10 LCEN, art. 6-1-7 : « *Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. […]* »

11 L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

12 https://www.internet-signalement.gouv.fr

b) Les suites données aux signalements

La plateforme PHAROS est le guichet unique des autorités. Son rôle est d'analyser les infractions en ligne, les qualifier, et judiciariser les contenus illégaux. Elle 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[13], OCRVP[14], etc.). Pour les affaires à dimension internationale, PHAROS se rapproche de l'agence INTERPOL.

Les signalements n'ont pas valeur de plaintes, mais de renseignements. Ils sont exploités selon la procédure suivante :

- 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 (exemples : sauvegarde des contenus et des éléments d'enquête, enrichissement et recoupement d'informations, vérifications techniques, investigations en source ouverte[15], intégration et comparaison d'images dans la base de données du CNAIP[16]), 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).

Quand le retrait du contenu ne peut pas être obtenu, PHAROS dispose d'une compétence exclusive de blocage administratif[17] pour les contenus pédopornographiques et de propagande terroriste, permettant d'empêcher tout accès à ces contenus par l'intermédiaire des fournisseurs d'accès à Internet (FAI) français. Cette procédure de blocage est contrôlée par la personnalité qualifiée de la CNIL[18].

---

13 Centre de lutte contre les criminalités numériques du Pole judicaire de la gendarmerie nationale

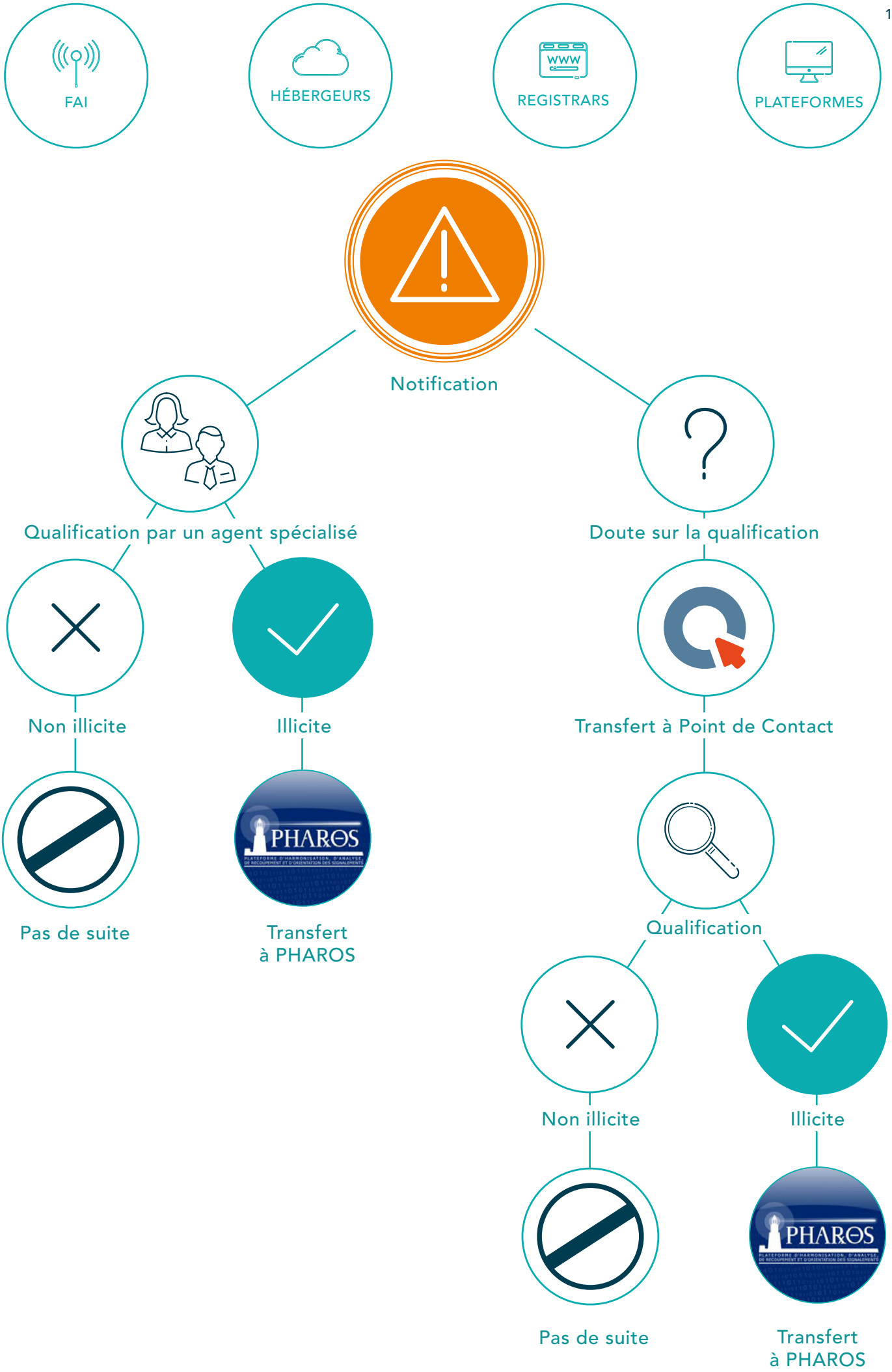
14 https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Office-central-pour-la-repression-des-violences-aux-personnes

15 Wikipédia : *« Le renseignement de sources ouvertes ou renseignement d'origine source ouverte (en anglais : open source intelligence, OSINT) est un renseignement obtenu par une source d'information publique. »*, https://fr.wikipedia.org/wiki/Renseignement_d%27origine_source_ouverte

16 Centre National d'Analyse d'Images Pédopornographiques, intégré au C3N, https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite

17 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id

18 https://www.cnil.fr/fr/controle-du-blocage-administratif-des-sites-la-personnalite-qualifiee-presente-son-3eme-rapport


FAI
HÉBERGEURS
REGISTRARS
PLATEFORMES
Notification
Qualification par un agent spécialisé
Doute sur la qualification
Non illicite
Illicite
Transfert à Point de Contact
Pas de suite
Transfert
à PHAROS
Qualification
Non illicite
Illicite
Pas de suite
Transfert
à PHAROS

B) Les actions et délais applicables

Lorsqu'un contenu manifestement 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 un délai raisonnable aux autorités pour procéder aux constatations nécessaires. Il est conseillé d'indiquer aux autorités la date et l'heure à laquelle la suspension sera effectuée.** Si possible, il est recommandé de mettre en place des espaces de délestage afin de conserver les contenus le temps nécessaire aux constatations policières.

Il convient donc de **suspendre le contenu ou de le rendre inaccessible, mais de ne surtout pas l'effacer**. Cette pratique est passible des sanctions prévues à l'article 434-4 du Code pénal[19]. L'hébergeur pourrait se voir reprocher d'avoir détruit des preuves et fait entrave à l'enquête.

Il faut bien garder à l'esprit que c'est dans les premières heures de leur présence en ligne que de tels contenus causent le plus grand tort, en raison de la vitesse à laquelle ils se propagent.

---

19 Art 434-4 Code pénal : *« Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, en vue de faire obstacle à la manifestation de la vérité :*

1° De modifier l'état des lieux d'un crime ou d'un délit soit par l'altération, la falsification ou l'effacement des traces ou indices, soit par l'apport, le déplacement ou la suppression d'objets quelconques ;

2° De détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.

Lorsque les faits prévus au présent article sont commis par une personne qui, par ses fonctions, est appelée à concourir à la manifestation de la vérité, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende. »

III) LA PROTECTION DES PROFESSIONNELS

L'exposition à ces contenus nécessite un aménagement adéquat des conditions de travail et un encadrement psychologique pour protéger les professionnels et les aider à maintenir leur équilibre personnel.

A) L'aménagement des conditions de travail

a) L'environnement de travail

Le traitement de ces contenus nécessite un aménagement spécifique de l'espace de travail. Les membres du personnel qui ne sont pas habilités à traiter ces contenus, et toutes les personnes amenées à être présentes dans les locaux, ne doivent en aucun cas être susceptibles d'y accéder, de les visualiser ou de les entendre.

Les ordinateurs servant à l'analyse de contenus devraient être a minima protégés par des mots de passe complexes et non accessibles[20]. En complément de cette sécurisation, il est recommandé de chiffrer ces machines. Par ailleurs, il est conseillé d'assortir les écrans de filtres de confidentialité et de les orienter de manière à ne pas exposer les autres salariés. Un casque audio est recommandé pour évaluer les bandes-son des vidéos, si nécessaire.

Les locaux, ou espaces dédiés, devraient également être signalisés par un avertissement interdisant l'accès aux professionnels 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.

Néanmoins, et malgré ces contraintes d'aménagement, 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.

La tendance actuelle est au développement du télétravail[21], néanmoins, il est fortement déconseillé de procéder au traitement de ces contenus en dehors des locaux prévus à cet effet. Associer l'espace que constitue le domicile personnel à un environnement d'images violentes peut nuire au salarié et à son entourage.

b) Les conditions de travail

Le professionnel qui analyse ces contenus ne devrait pas travailler seul dans un bureau. L'isolement peut accroître le stress lié à l'exposition aux contenus.

---

20 https://www.cybermalveillance.gouv.fr/wp-content/uploads/2018/09/Fiche-pratique-mots-de-passe.pdf

21 https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072050&idArticle=LEGIARTI000025558060

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

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.

B) La psychologie au cœur du métier

Les effets de ces métiers sur la santé psychologique sont souvent minimisés par les professionnels exposés par fierté, pudeur, manque d'attention à soi, ou manque de sensibilisation aux effets insidieux engendrés par le traitement de ces contenus choquants.

Important : pour l'entreprise ou la puissance publique, il convient 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. Il n'existe pas de règles absolues en matière de résilience psychologique. 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.

a) L'entretien psychologique : une démarche souhaitable avant d'exercer

Protéger les professionnels, c'est d'abord s'assurer de leur capacité à supporter l'exposition à ces contenus. Il est recommandé de faire passer un entretien psychologique à tout candidat ou salarié pressenti pour occuper un poste comportant une telle exposition.

Cet entretien préalable à la mission doit être réalisé par un psychologue clinicien ou un psychologue du recrutement. 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. L'avis du psychologue ne lie pas le recruteur mais lui permet cependant 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.

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

b) Un suivi psychologique tout au long de la mission

Une fois la personne recrutée, il est vivement conseillé de mettre en place un suivi psychologique obligatoire que seul un psychologue clinicien est en mesure de réaliser. Le psychologue du travail spécialisé dans la prévention des risques psycho-sociaux peut se situer dans l'accompagnement du chef de service ou de structure dans la prise en compte des situations évoquées par les professionnels à des fins de prévention. La fréquence des entretiens psychologiques obligatoires devrait être supérieure à un entretien annuel. Alternativement à ce suivi obligatoire, le professionnel exposé doit pouvoir avoir accès à une consultation lorsque le besoin s'en fait sentir, sans avoir à obtenir l'accord préalable de son employeur. Ces consultations devraient être prises en charge intégralement par l'entreprise. Tous les salariés, quelle que soit leur ancienneté, doivent pouvoir bénéficier du même suivi.

La demande d'entretien ne devrait jamais être utilisée pour douter des capacités du professionnel à poursuivre sa mission. L'entretien doit être confidentiel afin de permettre un échange libre entre le salarié et l'entité en charge du suivi psychologique. Néanmoins, le psychologue en charge du suivi doit pouvoir alerter la structure en cas de risque pour le professionnel et/ou pour la structure, tout en respectant la confidentialité des entretiens. À 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 du suivi des équipes doivent veiller à prendre toutes les mesures pour assurer leur accompagnement et leur protection.

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

Des entretiens collectifs peuvent aussi être d'une grande valeur pour améliorer le travail d'équipe et construire une réflexion collective.

Important : demander un entretien psychologique en dehors du suivi obligatoire ne devrait jamais être considéré comme un aveu de faiblesse ou un indicateur d'incapacité. Bien 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.

c) Un entretien en fin de mission

Lorsqu'un professionnel achève sa période de travail en présence de contenus pédopornographiques et/ou d'images d'exactions violentes, 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. Il est conseillé de faire un entretien psychologique au moment où le salarié 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.

Le regard d'une psychologue spécialisée

Exposition des professionnels à des contenus potentiellement traumatiques

Par Camille Peninon

Psychologue clinicienne – Psychothérapeute, spécialisée en psychotraumatisme et interculturel. Intervenante pour Point de Contact depuis janvier 2019.

« L'exposition à des contenus potentiellement traumatiques – de façon répétitive et sur du long terme/qu'ils soient qualifiés de pédopornographiques ou de propagande terroriste – confronte nécessairement les professionnels à la question de la solidité du cadre.

Le « cadre » est à entendre à deux niveaux, extérieur et intérieur. D'une part, il s'agit d'un aménagement particulier des conditions et de l'environnement de travail comme évoqué dans ce Livre Blanc ; cet axe pourrait être considéré comme un devoir de protection de l'employeur envers les professionnels. D'autre part, il s'agit aussi du cadre interne à chaque professionnel, de la stabilité de son équilibre psychique et des conditions pour protéger ce dernier ; cet axe, lui, pourrait être compris comme un devoir de protection de soi envers soi-même. Par ailleurs, la « solidité du cadre » est à entendre en ce sens qu'il doit être contenant/étayant/rassurant, mais aussi qu'il doit pouvoir résister/tenir/s'adapter si besoin.

Dans cette pratique spécifique que constitue l'analyse de contenus potentiellement traumatiques, le cadre interne semble régulièrement être questionné, bousculé, mis à mal. De plus, cet effet semble parfois minimisé/banalisé par les professionnels eux-mêmes. Les situations professionnelles nécessitent donc une prise de distance face aux contenus ainsi qu'à leurs possibles conséquences. L'accompagnement psychologique vise à permettre une prise de conscience des éventuelles répercussions des missions, une identification de certaines émotions, un partage de celles-ci ainsi que leur élaboration. Le professionnel doit faire le travail de bien se connaitre, d'identifier ses domaines de sensibilité et de les respecter, d'être à l'écoute de ses mouvements internes et ne pas rester seul, isolé avec ces derniers. Il s'agira de les partager avec les collègues et les responsables, au cours de réunion d'équipe mais aussi de temps informels ; il parait bénéfique aussi de le verbaliser auprès du psychologue.

Les risques psychologiques de la confrontation à des contenus potentiellement traumatiques peuvent être multiples : minimisation, banalisation, sidération, fascination, tristesse, anxiété, trauma vicariant, trauma secondaire, identification à des victimes, sentiments de culpabilité et d'impuissance, ruminations anxieuses sur les suites judiciaires des contenus traités, burn-out… Rappelons une chose fondamentale : il n'est pas normal de s'habituer à l'anormal, à l'inhumain, à l'insupportable. »

ANNEXE : RESSOURCES DOCUMENTAIRES

Définitions et répression de la pédopornographie :

Convention sur la cybercriminalité, Conseil de l'Europe, 2001, https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680081 56d

Convention sur la protection des enfants contre l'exploitation et les abus sexuels, Conseil de l'Europe, 2007, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084833

Réseau international de points de signalement INHOPE, https://www.inhope.org/EN, https://www.inhope.org/EN/articles/child-sexual-abuse-material

Internet Watch Foundation (IWF), https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels

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

Child Sexual Abuse Material, Model Legislation and Global Review, International Centre For Missing and Exploited Children, 9e edition, 2018, https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf

Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels, Adopté par le Groupe de Travail Interinstitutionnel sur l'exploitation sexuelle des enfants en janvier 2016, ECPAT International et ECPAT Luxembourg, Mars 2017, http://luxembourgguidelines.org/fr/version-francaise/

Guides de bonnes pratiques sur la protection des professionnels :

MAAWG Disposition of Child Sexual Abuse Materials Best Common Practices, Messaging Malware Mobile Anti-Abuse Working Group, February 2015, https://www.m3aawg.org/sites/default/files/document/M3AAWG_Disposition_CAM-2015-02.pdf

Employee Resilience Guidebook for Handling Child Sexual Abuse Images, The Technology Coalition, January 2015, Version Two, https://static1.squarespace.com/static/5539d022e4b0a048151fd-94b/t/57a820f02e69cff-b1a382a7b/1470636275925/TechnologyCoalitionEmployeeResilienceGuide-bookV2January2015.pdf

Ce document est une réactualisation proposée par l'association Point de Contact du *Guide d'Usage pour la Lutte Contre la Pédopornographie*, rédigé en 2014 à l'initiative d'Alexandre Hugla, responsable du service abuse de Gandi.net.

Disclaimer :

Ce document a été actualisé et republié en février 2020 avec le soutien financier de la DG Justice *(Rigths, Equality and Citizenship (REC) Programme)* de l'Union européenne, dans le cadre du projet *Click@ble – Make children able to "click" free from cyber sexual violence*[22]. Le contenu de ce document relève de la seule responsabilité de Point de Contact et ne peut en aucun cas être vu comme reflétant les opinions de l'Union européenne.

Comité de rédaction :

Quentin Aoustin,
Directeur des Opérations,
Association Point de Contact

Alexandre Archambault,
Avocat à la Cour, spécialiste du droit des nouvelles technologies de l'information et de la communication

Philippe Baudoin,
Colonel de Gendarmerie,
Conseiller, Ministère de l'Intérieur – DMISC,
Mission de Lutte contre les cybermenaces

Adeline Champagnat,
Commissaire divisionnaire de la police judiciaire,
Direction centrale de la police judiciaire,
Conseiller à la délégation en charge de la lutte contre les cybermenaces

Caroline Claux,
Capitaine de Gendarmerie,
Chef de Département au Centre de lutte Contre les Criminalités Numériques (C3N) du Service Central de Renseignement Criminel de la Gendarmerie Nationale

Alain Doustalet,
Responsable Service Abuse, Orange

Florence Esselin,
Conseiller expert en numérique et cybersécurité,
Direction générale de la Gendarmerie Nationale – Cabinet, Mission numérique de la Gendarmerie Nationale

Thomas Fontvielle,
Secrétaire Général, Association Signal Spam

Alexandre Hugla,
Responsable Service Abuse, Gandi.net

Jean-Christophe Le Toquin,
Président, Association Point de Contact

Nikoleta Lydaki Simantiri,
Juriste – Analyste, Association Point de Contact

Patrick Mariatte,
Commandant de Police, Chef de la section Internet de l'OCLCTIC

Camille Peninon,
Psychologue clinicienne – Psychothérapeute, spécialisée en psychotraumatisme et interculturel

Anne Souvira,
Chargée de mission « Cyber », Cabinet du Préfet de Police, Préfecture de Police de Paris, Ministère de l'Intérieur

---

22 En français le titre du projet signifie « *Renforcer la capacité des enfants à "cliquer" à l'abri des violences sexuelles en ligne* ». Pour plus d'information, https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2019/08/Fiche-projet_CLICK@BLE.pdf