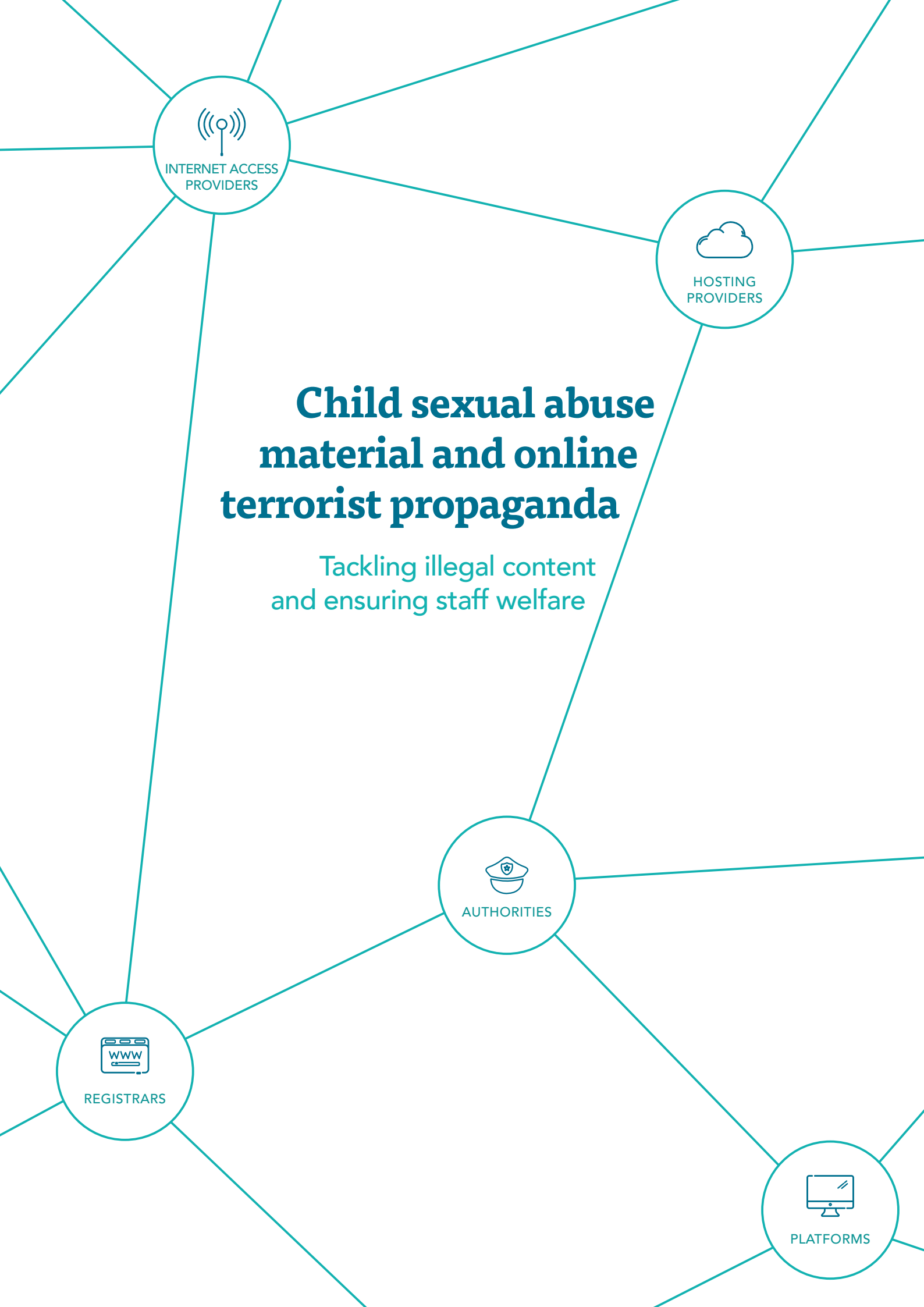


Child sexual abuse material and online terrorist propaganda

Tackling illegal content and ensuring staff welfare

TABLE OF CONTENTS

FOREWORD – PURPOSE AND SCOPE

This white paper aims to develop a shared set of best practices pertaining to the operational handling and processing of harmful and potentially illegal content, which may endanger the physical safety and psychological wellbeing of professionals.

The illegal and harmful content mentioned here refers to two separate categories: Child Sexual Abuse Material[1] (article 227-23 of the French Criminal Code) and content which incites or advocates committing terrorist offences (article 421-2-5 of the French Criminal Code).

While there has been a continuous growth in the distribution of and access to such content since the 1990s, one can only observe that there has been an acceleration since 2010, with the spread of connected devices (tablets, smartphones, smart TV sets, video game consoles) and high-speed, mobile broadband networks.

Therefore, these past few years, the number of individuals tasked with handling and processing such content worldwide has grown exponentially, reaching several thousand today. Small and medium enterprises (SMEs), as well as larger corporations, are compelled to be equipped with services dedicated to this activity. Even if technology and artificial intelligence boost the effectiveness of these professionals, the sheer complexity of content assessment and the very issue of protecting people from harm continue to stress the necessity of human intervention.

The present handbook is aimed at professionals from companies which publish and distribute online content, hosting providers and platforms, social media, domain name registrars, Internet access and service providers, law enforcement authorities as well as all staff members whose responsibility and function is to tackle illegal content resulting from cybercrime activities.

The protection of victims who appear in such content, as well as the protection of individuals who may be targeted by such content, call for the intervention of qualified professionals. This is precisely why it is essential to come up with a shared set of best practices to strengthen the effectiveness of reporting loops.

Harmful content may affect all those who are exposed to it in their professional capacity, whether on a regular or periodic basis. Because those professionals make up an essential first line of defence, this white paper intends to contribute to acknowledge their role and the necessity to take steps to ensure their welfare.

---

1 We prefer the use of the term Child Sexual Abuse Material abbreviated as CSAM to refer to content elsewhere referred to as 'child pornography'. The use of the term "child pornography" in relation to children is criticised, as "pornography" is a term primarily used for adults engaging in consensual sexual acts, instead of highlighting the fact that children are victims of sexual abuse and/or sexual exploitation. The term "child sexual abuse material" (CSAM) is increasingly being used to replace the term "child pornography" highlighting the fact that children are victims and that the acts are carried out without their consent/responsibility. For more information regarding terminology, see resources in the annex of this document.

I) RECEIVING REPORTS

The French Law regarding Trust in the Digital Economy (*La loi pour la confiance dans l'économie numérique*, LCEN)[2] stipulates that all hosting providers, whether natural persons or legal entities, should contribute to the fight against content which incites or advocates committing terrorist offences, as well as child sexual abuse material, as types of illegal and harmful content.

The primary positive obligation which relies upon them may be found at article 6 – I, paragraph 7:

"[…] As such, they must put in place a visible and easy-to-access reporting tool which allows any person to bring to their attention the existence of such content. They also have the obligation, on the one hand, to promptly inform the competent public authorities of all illicit activities mentioned in the previous paragraph, should they be reported to them […]"

A) The reporting mechanism

a) Setting up a reporting tool

The first obligation is to provide the public with an easy-to-access online reporting tool so it takes no more than a few clicks to fill out and complete the complaint form. To this end, a dedicated, simple, easily identifiable and free of charge reporting mechanism should be set up. Publicly accessible content should be reported without having to create an account. It is also recommended to offer Internet users the possibility to report content anonymously.

A reporting mechanism is often materialised by an email address e.g. abuse@example.tld or, via a dedicated online form. For edited content on platforms, Internet users should be able to report suspected illegal content at any time throughout their browsing session on the platform.

It is strongly advised that the reporting channel be entirely and solely dedicated to this use in order to separate this information from other exchanges (e.g. requests directed to the sales department, consumer complaints, enquiries).

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

b) Receiving reports

Receiving and handling potentially illicit content should only be reserved for authorised employees tasked with content assessment. Likewise, other employees who are not assigned with content assessment should not be exposed to such content. Reviewing such content absolutely requires the prior consent of the affected employee(s) and should under no circumstances be imposed upon them arbitrarily.

B) Assessing content

a) Assessing child sexual abuse material

Child sexual abuse material and its online distribution[3] are referred to in article227-23 of the French Criminal Code. Paragraph 1 stipulates:

"Taking, recording or transmitting an image or representation of a minor with a view to circulating it, where that image or representation has a pornographic character is punished by five years of imprisonment and a fine of 75,000 euros. When that image or representation regards a minor under fifteen years of age, these offences are punished, even if they were not committed with a view to circulating the image or representation."

Paragraph 1 specifies the content referred to as depicting minors, that is to say any person under the age of eighteen. While determining if a person is a minor is in general not difficult, the distinction between a minor and an adult is not always obvious, especially for adolescents.[4]

The French legislation does not distinguish between real or virtual content (e.g. drawings, photomontages or photoshopping). In France, only fictional text describing child sexual abuse or advocating paedophilia is not covered by law.

The content must be of sexual nature. This excludes a priori from the former images of nudism or naturism, as well as images of naked or semi-naked children in a non-sexualised context. By contrast, this includes all images of children, naked or clothed, where the analysis of the wider context, the characteristics of the shooting, specific focus on certain parts of the body, the child being made to pose in an inappropriate way, or toys or objects suggesting a sexually explicit setting may guide the assessment.

Therefore, by considering the context, an image depicting a naked child may be legal while an image depicting a clothed child may be illegal.

---

3 Art 227-23 al.2: *"The penalties are increased to seven years of imprisonment and fine of 100, 000 euros when use was made of a communication network for the circulation of messages to an unrestricted public in order to circulate the image and representation of a minor."*

4 For further information, The Tanner scale provides a classification of the various stages of puberty development.

The last paragraph of article 227-23 makes the following clarification:

"The provisions in the present article shall also apply to pornographic images of any person whose physical appearance is that of a minor, unless it is proven that the person was over eighteen years of age on the day the image was taken or recorded."

The article stipulates that images of a person whose physical appearance is that of a minor should also be subject to the full force of the law. What is relevant here is visual depictions that *"appear to be"* of minors. **When in doubt as per the age of the depicted person, it is advised to report the content.**

French law does not provide an accurate definition of what is meant by an image or representation of 'pornographic nature' of a minor, but other sources[5] might prove insightful in this regard.

Directive 2011/93/EU[6] of the European Parliament and the Council of 13 December 2011 states in its definitions reported in Article 2:

"[…] c) 'child pornography' means:

i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

ii) any depiction of the sexual organs of a child for primarily sexual purposes;

iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or

iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes; […]"

b) Assessing terrorist propaganda

The first two paragraphs of article 421-2-5 of the French Criminal Code address the legal framework and scope of the offences:

"Directly inciting to the committing of terrorist acts or publicly advocating the committing of such acts are punished by five years of imprisonment and a fine of 75,000 € . The punishment shall be seven years of imprisonment with a fine of 100,000 € if the offences are committed while using an online public communication service."

---

5 To help you in assessing child sexual abuse material, you may find useful sources and links listed in the annex of the present document.

6 https://publications.europa.eu/en/publication-detail/-/publication/d20901a4-66cd-439e-b15e-faeb92811424/language-en

How to comprehend what does or does not qualify as incitement to terrorism or advocacy of terrorism?

The official website of the French public administration sheds light on the matter in a factsheet covering such offences:[7]

> *"Advocacy/glorification of terrorism*
>
> *Advocacy or glorification of terrorism consists in presenting or commenting favourably on terrorist acts which have already been committed. For instance, if a person approves of a terrorist attack.*
>
> *Advocacy or glorification differs from terrorism denial. Denying terrorist acts is when a person partially or completely denies these acts ever took place, without directly condoning them. For instance, if the person invokes a conspiracy.*
>
> *To be punishable by law, advocacy or glorification means it was carried out publicly. The public nature of the statements may be assessed in the same way as for defamation and insult. Therefore, comments made on publicly accessible social media may be punished.*
>
> *Incitement to terrorism*
>
> *Incitement to terrorism means direct incitement or provocation to commit materially determined terrorist acts. For instance, to deliberately target a location or a well-known public figure. With regard to the context, the intentionality of the author and the chosen wording, such statements are intended to encourage and persuade other people to commit such acts.*
>
> *Here, it is a matter of incitement, encouragement to carry out acts of terrorist nature in the future and not an endorsement and approval of terrorist acts which have already been committed.*
>
> *Such statements do not need to have been made in front of a large audience. Comments which may be read by a few friends on social media or made during a private meeting may be punished."*

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

Terrorist propaganda which does not include violent imagery may be illegal. **The context has a bearing on the assessment.** Researchers and journalists may use this kind of content to illustrate the findings of their investigations. It is therefore advisable to differentiate publications which are intended to denounce terrorist propaganda, which shall not be subject to the force of the law, from publications which are intended to promote terrorism, and which shall be classified as incitement to or glorification of terrorism.

Besides, harmful content depicting scenes of brutal violence, and not falling under the categories of incitement to or glorification of terrorism, may nevertheless prove illegal, by constituting, for instance, a violation of human dignity.

Beyond direct incitement to committing acts of terrorism or the glorification of terrorist attacks which have already been carried out, anything which is intended to lead people to adopt the ideology of a given terrorist group, to join their ranks, as well as any kind of publicity designed to promote it should also be identified and assessed as illegal content.

Because of the language used in certain publications, it may at times be difficult to understand certain content and therefore assess it or determine whether it is illegal. In such cases, **it is highly recommended to report any content which includes emblematic visual signs that directly link the content to a known terrorist group, or one of its media.**

II) PROCESSING REPORTS

The mission of employees tasked with processing reports is to assess and determine whether the content is manifestly illegal according to French law. If the assessment seems obvious in many cases, certain content may raise questions. When in doubt, it is advised to forward the reports to the competent authorities who will proceed with assessing their legality, or to contact, for instance, the professional association *Point de Contact*,[8] the private sector platform dedicated to the processing of reports of suspected illegal online content.

A) Forwarding reports to the authorities

a) PHAROS[9]: the national portal to report illegal online content

The second obligation for content hosting providers is to promptly inform law enforcement authorities as soon as they are aware of manifestly illegal online content hosted on their sites. The French LCEN does not impose upon the hosting provider a general obligation of surveillance as per the information/data it transmits or stores[10] but, as soon as the hosting provider becomes aware of the presence of a publication which is manifestly illegal on its sites, it should promptly inform law enforcement authorities.

In order to receive reports and tip-offs from the general public and Internet stakeholders, the French authorities also set up a dedicated unit. Thus, the PHAROS platform, staffed by gendarmes and police officers, was set up on September 1st, 2006 within the OCLCTIC,[11] France's national cybercrime investigation unit, to ensure the judicial processing of the reports.

An online form[12] has been made available to the public and allows anyone to report suspicious online content or behaviour. Private entities can sign a partnership agreement with the platform to obtain a *trusted flagger* account.

---

8 https://www.pointdecontact.net/

9 In French, the acronym stands for *Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements* (Platform for the Harmonisation, Analysis, Cross-checking and Orientation of Reports)

10 LCEN, article 6-1-7. "The persons mentioned in 1 and 2 are not subject to a general obligation of monitoring the information they transmit or store, nor to a general obligation of looking for facts and circumstances that reveal unlawful activities […]"

11 in French, the acronym stands for *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* (Central Office for Combating Information and Communication Technology Crime)

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

b) Follow-up of reports

The PHAROS platform is the French authorities' single entry point. Its role is to analyse and assess online offences, with further legal action for illegal content. It redirects the reports towards the locally competent law enforcement authorities, whether the police or the gendarmerie, or towards specialist services depending on the nature of the content (C3N,[13] OCRVP,[14] etc.). For matters involving international cooperation, PHAROS works closely with INTERPOL.

Reports are not considered as complaints, but rather as tip-offs or leads. They are used as the following procedure shows:

- checking the existence of the reported content (is it still online?);
- legal assessment (is it illegal according to French law?);
- precautionary measures (e.g. content back-up and evidence archiving, enhancement and cross-checking of information, technical verifications, OSINT,[15] image integration and image comparison in the CNAIP[16] database, etc.), deciding upon the competent authority (if necessary, with additional investigative capabilities);
- start of an investigation.

OR

- forwarding of reports to the competent authority, police or gendarmerie unit, or to the competent authority abroad via INTERPOL;
- start of an investigation by the competent authority;
- follow-up (advice to the competent authority and feedback).

When content removal cannot be obtained, PHAROS has exclusive competence over administrative blocking[17] for child sexual abuse material and terrorist propaganda, blocking all access to these publications via the French Internet service providers. These measures are subject to oversight by the designated person of the French Data Protection Authority, the CNIL.[18]

---

13 The acronym stands for *Centre de lutte contre les criminalités numériques* (Central Unit for Fighting Digital Crime), which operates within the French Gendarmerie.

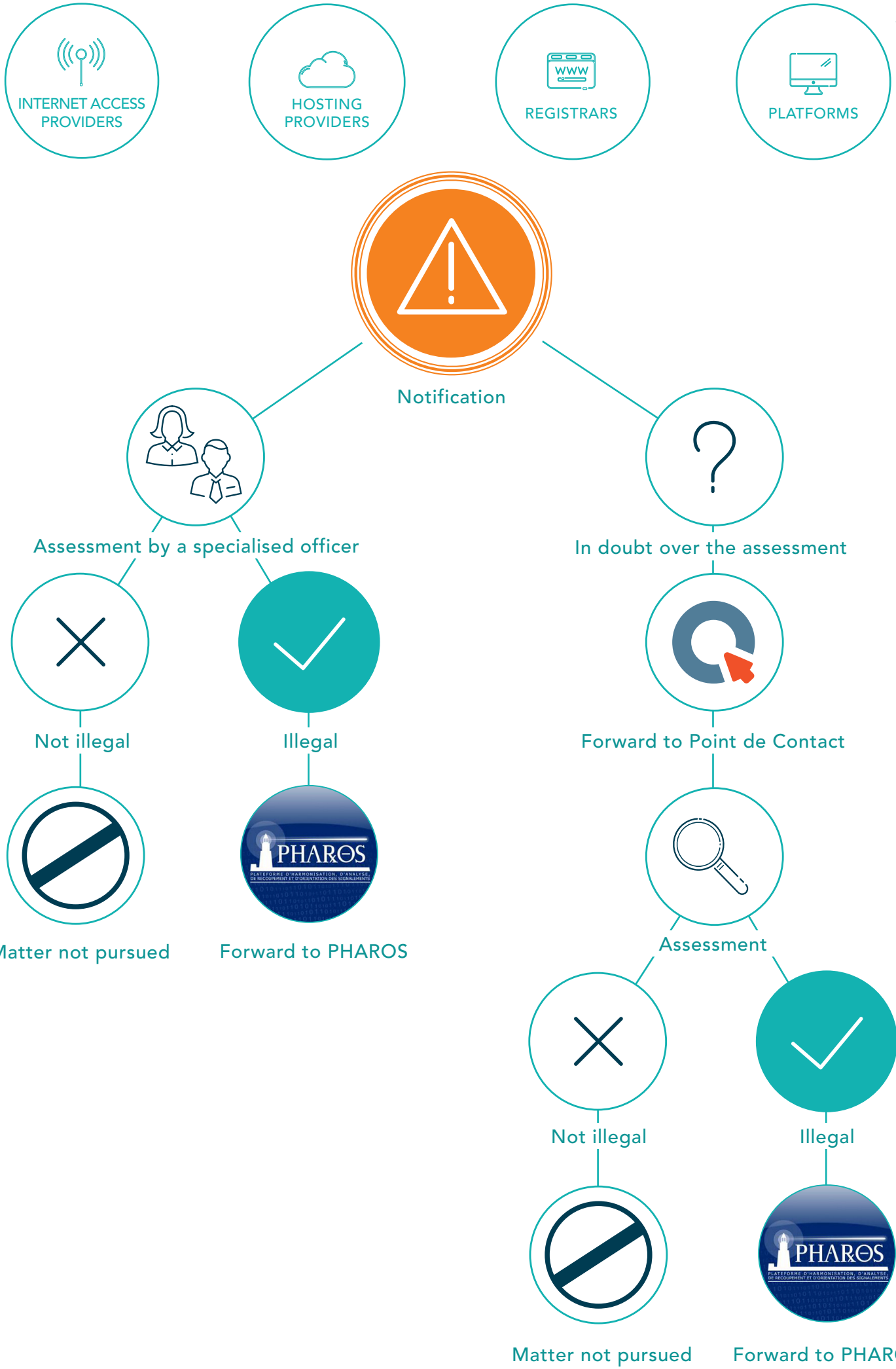
14 https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Office-central-pour-la-repression-des-violences-aux-personnes

15 Wikipedia: "Open-source intelligence (OSINT) is data collected from publicly available sources." https://fr.wikipedia.org/wiki/Renseignement_d%27origine_source_ouverte

16 In French, the acronym stands for *Centre National d'Analyse d'Images Pédopornographiques* (National Centre for the Analysis of Child Sexual Abuse Images) 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


INTERNET ACCESS PROVIDERS
HOSTING PROVIDERS
REGISTRARS
PLATFORMS
Notification
Assessment by a specialised officer
In doubt over the assessment
Not illegal
Illegal
Forward to Point de Contact
Matter not pursued
Forward to PHAROS
Assessment
Not illegal
Illegal
Matter not pursued
Forward to PHAROS

B) Applicable actions and time limits

When manifestly illegal content is reported to the hosting service provider, it must, after assessment, expeditiously notify the competent authorities and forward it to them. Then, it must disable the online content from public access, **while allowing sufficient time for police investigations and digital forensics. It is advised to indicate the date and time by which the suspension will take place.** If possible, it is recommended to set up a dedicated offloading space, to preserve the content during the time necessary for the investigation.

The content should therefore **be suspended or made inaccessible**, but should **certainly not be deleted.** Such a procedure is subject to the relevant criminal penalties, as per the article 434-4 of the French Criminal Code.[19] The hosting provider could be accused of destroying evidence and jeopardising the ongoing investigation.

It should be noted that it is right from the beginning, from the very first hours of online presence, that such content is most harmful, due to how quickly it spreads.

---

19 Article 434-4 of the French Criminal Code: *"Where it is done to in order to obstruct the discovery of truth, a penalty of three years of imprisonment and a fine of 45,000 euros applies to:*
1° Modifying the scene of a felony or misdemeanour either by the alteration, falsification or obliteration of clues and evidence, or by bringing, removing or suppressing any given object;
2° Destroying, purloining, concealing, or altering a private or public document or an object to facilitate the discovery of a felony or misdemeanour, the search for evidence or the conviction of the guilty party.
Where the acts provided for under the present article are committed by a person who, because of their position, is called to take part in the discovery of the truth, the penalty is increased to five years of imprisonment and a fine of 75,000 euros"

III) STAFF WELFARE

Exposure to such content requires a suitable working space set-up, appropriate working conditions, and psychological assessments to protect professionals and help them safeguard their personal wellbeing.

A) Setting up the workplace environment and establishing working conditions

a) Workplace environment

Processing such content requires a specific set-up and configuration of the employee's workstation. Employees who are not authorised to view content, and other people who might be in the premises, should in no circumstances be able to access, view nor hear such content.

Computers which are used for content assessment should, by default, be protected by complex and not accessible passwords. Besides this security procedure, it is highly recommended to have these computers encrypted. In addition, it is advisable to attach privacy filters to computer screens and position them so as to avoid any kind of content exposure to other employees. The use of headphones is also recommended to assess video sound, if necessary.

The facilities, or dedicated spaces, should also be signalled by a warning sign to prohibit entry to unauthorised personnel.

If remote work is on the rise and trending,[20] it is nonetheless strongly inadvisable to review and assess content outside facilities intended for this purpose. To associate one's home with an environment of violent imagery would be harmful and prejudicial to the employee and their loved ones.

Protecting the outside environment from exposure to content is also a measure which should be considered. Windows may be fitted with opacifying panels if the working space can be seen from the outside.

Nevertheless, and despite these set-up and configuration constraints, it must be ensured that professionals are not further isolated, so they do not feel excluded from the organisation's work environment.

b) Working conditions

The professional who assesses such content should not work alone in the office. Isolation can increase the stress related to content exposure.

---

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

The professional should be able to go for a break whenever they feel the need for it, when working on content assessment, so they can unwind, step back and distance themselves from content which might have shocked them.

It is recommended to set up a relaxation area in the office, outside the content assessment area, so one can more easily extract oneself from the content related environment. Certain entities provide video game consoles, board games, table football, TV, reading materials or offer sports and cultural activities.

The employee should be able to talk to their manager when needed or any competent person within the structure. It is advised to have regular team meetings during which working conditions may be re-evaluated.

B) Psychology at the heart of the job

The effects of this type of jobs on one's psychological health are often downplayed by the exposed personnel for reasons of pride, modesty, self-neglect or by a lack of awareness of the insidious effects of dealing with such harmful content.

Important: for the company or the public entity, generalisations or assumptions based upon one's age, gender or known marital and family status should not be made as per the ability of a person to deal with such content. There are no rules in terms of psychological resilience. For all individuals, the risks, such as psychological fatigue, are real and should be taken seriously, irrespective of the frequency or degree of exposure.

a) Prior psychological assessment: a desirable procedure before starting in the role

Protecting staff also means ensuring their ability to endure exposure to such content. It is highly recommended to have the candidate or employee considered for a job with such exposure undergo a psychological assessment.

Prior psychological assessment must be carried out by a clinical psychologist or a recruitment psychologist. The purpose of the assessment is to evaluate the awareness of the candidate as per their future duties and their potential consequences on their psychological wellbeing, as well as to judge their ability to work in the prolonged presence of potentially traumatic content. The psychologist's opinion should not bind the decision of the recruiter but may guide it. It should also be noted that prior psychological assessment may be valid in the moment and not prejudge psychological change which may be observed at a later stage in subsequent sessions.

Important: the in-house transfer towards a role as specific and particular as a content assessment one should always be consented to by the colleague, who must understand the range and risks of the job, and fully comprehend the recommendations to protect oneself.

b) Psychological follow-up throughout the working period

Once the person is hired, it is highly advised to set up compulsory psychological follow-up that only a clinical psychologist can carry out. The occupational psychologist specialised in the prevention of psychosocial risks may assist, for prevention purposes, the head of the department or the organisation in taking into account the situation at hand. The frequency of the mandatory psychological assessments should exceed one session per year.

On top of this mandatory follow-up, the exposed professional should have access to counselling when needed, without the employer's prior consent. The cost of these counselling sessions should be entirely covered by the company. All staff members, irrespective of their seniority and length of service, should benefit from the same follow-up.

A request for a counselling session should never be used to doubt the ability of the professional to perform their duties. The session should be confidential to allow for open dialogue between the employee and the entity in charge of the psychological follow-up. However, the psychologist in charge of the follow-up should be able to alert the organisation when there is a risk for the professional or the organisation, while respecting the confidentiality of the sessions. At a minimum, the psychologist should be able to alert the organisation via the occupational physician of the need to review how content is being processed as well as of the necessity to pay attention to the psychological health of the exposed personnel. The psychologists in charge of the follow-up of these personnel should make sure all steps and measures are taken to ensure their support and protection.

It may occur that a professional is unable to find themselves in need of psychological help or that they do not sufficiently take into account the risks that their state might generate. It may be considered useful to heighten the awareness of the line managers as per the detection of early signs of psychosocial risks, possibly with the help and intervention of an occupational physician.

Group counselling sessions might also prove highly valuable to improve teamwork and build shared awareness.

Important: requesting a counselling session outside the mandatory follow-up should never be perceived as a sign of weakness or an indicator of unsuitability for the job. On the contrary, the professional who knows how to identify when their wellbeing might be threatened, and who takes the initiative to avoid related risks, is much more equipped to carry out their duties in good conditions than the person who chooses not to divulge the encountered difficulties.

c) Final assessment upon leaving the job

When a professional ends their work period in the presence of child sexual abuse content and/or images of scenes of terror, it will not mean that the images and videos they were exposed to will leave their mind. The professional may have experienced episodes of psychological fatigue which, if left insufficiently treated, could well persist after the end of their contract. Profound alteration may have taken place in terms of moral, philosophical, spiritual or political representations and conceptions. It is advised to carry out a psychological assessment when the professional leaves their job. This assessment should allow the professional to take stock of this professional experience, to mention what may have affected them in both professional and private spheres, and to detect any consequences it may have had on them. The psychologist should be able to provide guidance as per dealing with potential difficulties, or respond to certain questions, which may remain or resurface in the future.

Insights from a specialised psychologist

Psychological aspects of the professional viewing child sexual abuse images

By Jean-Baptiste Colle

Graduate from the French School of Practising Psychologists, specialised in criminology, psychotrauma and child protection. In charge of psychological follow-up for the association *Point de Contact* from 2014 to 2018.

« Viewing images or videos of child sexual abuse is never harmless. Within the company, the person in charge of assessing such content should have volunteered and chosen, beforehand and out of free will, to carry out such a delicate mission, be trained in content analysis, and receive throughout the process support from a colleague or a line manager. When dealing with such content, it is important that the individual is not alone and can talk to another colleague who will be able to provide support, guidance and even assistance with filing the report.

When facing such imagery, the analyst may feel alternately confusion, fascination, astonishment, rejection, an absence of affect, anxiety, sadness, guilt, shame, and even a profound questioning of one's very own ideals and conceptions which guide both one's inner world and outlook on society.

The confrontation with such raw, harsh images depicting child sexuality takes us back to our representations of child and adult sexuality, as well as sexual violence. We are not all equipped with the same mental and psychological resources, as per our history (past history of intra- or extra-familial sexual violence, unsatisfying sexual experience…) as well as our current emotional and family life (parent of young children, current pregnancy, going through a difficult patch…). The analyst may at times feel useless, lonely, not feeling heard or understood, and this, possibly in echo to the experience and feelings that a child victim or an adult sex offender could have.

Indeed, it is possible that a 'transfer' to or an 'identification' with one of the protagonists depicted in a video or an image may take place. This frequent mechanism, allowing the subject to 'be in someone else's shoes', may be experienced with anxiety, and should be worked upon in a different space, with a psychologist, to identify the emotions, thoughts and representations which the subject associates with these images. This may also help the subject to understand the function of one's job with regard to current society, distance oneself, as well as drawing a line between work and private life. »

ANNEX: RESOURCES

Legal definitions and the fight against child sexual abuse material (CSAM):

Convention on Cybercrime, (definition at article 9 §2), Council of Europe, 2001
http://www.europarl.europa.eu/meet-docs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Convention on the Protection of Children from Sexual Exploitation and Sexual Abuse (definition at article 20 §2), Council of Europe, Lanzarote, 2007
https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97

The International Association of Internet Hotlines, INHOPE:
http://inhope.org/gns/internet-concerns/overview-of-the-problem/child-pornography.aspx

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

Child Pornography: Model Legislation and Global Review, ICMEC, 8th edition, 2016
http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf

Crimes against children - INTERPOL:
https://www.interpol.int/en/Crime-areas/Crimes-against-children/Crimes-against-children

Documentation on terminology:

Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group on Sexual Exploitation of Children, 2016
http://luxembourgguidelines.org/english-version/

Other handbooks on best practices:

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

Staff Welfare Best Practice Paper, INHOPE 2013
http://hotlinedevelopmentguide.org/cms/wp-content/uploads/2016/04/Best-Practice-Staff-Welfare-2013.pdf

Employee Resilience Guidebook for Handling Child Sexual Abuse Images, The Technology Coalition, 2013
http://technologycoalition.org/wp-content/uploads/2013/05/EmployeeResilienceGuidebook2013.pdf

The present document is an update provided by the French Association *Point de Contact* of the *Guide d'Usage pour la Lutte contre la Pédopornographie* (A Professional Handbook on the Fight against Child Sexual Abuse Material), drafted in 2014 upon the initiative of Alexandre Hugla, in charge of the anti-abuse department at Gandi.net.

Editorial Board :