COMMISSION
EUROPÉENNE

Bruxelles, le 16.12.2016
COM(2016) 872 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

évaluant la mise en œuvre des mesures visées à l'article 25 de la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie

Table des matières

1. INTRODUCTION

L'internet a provoqué une augmentation spectaculaire des abus sexuels d'enfants car:

- il facilite le partage de matériel ayant trait à des abus sexuels d'enfants, en offrant une variété de canaux de distribution tels que le web, les réseaux de pair à pair, les médias sociaux, les tableaux d'affichage, les forums de discussion, les discussions relayées par internet (IRC) et les plateformes de partage de photos, parmi beaucoup d'autres. Le partage est également facilité par l'accès à une communauté mondiale de personnes partageant les mêmes idées, source de forte demande et d'appui mutuel;
- il fournit des moyens techniques et des mesures de sécurité qui peuvent faciliter l'anonymat[1];
- en raison de la forte demande de matériel ayant trait à des abus sexuels d'enfants, les enfants continuent à être exposés au risque de devenir des victimes, tandis que l'anonymat est susceptible d'entraver le travail d'enquête et la poursuite de ces crimes; et
- les nouveaux matériels ayant trait à des abus sexuels d'enfants sont devenus une monnaie d'échange. Pour obtenir et conserver leur accès aux forums, les participants doivent souvent soumettre du matériel nouveau de manière régulière, ce qui encourage la commission d'abus sexuels d'enfants.

L'abus sexuel d'enfants en ligne est un crime abominable qui a des conséquences à long terme pour les victimes. Les dommages sont causés non seulement lorsque l'abus est effectivement enregistré ou photographié, mais aussi chaque fois que les images et les vidéos sont publiées, diffusées et consultées. Pour les victimes, le fait d'avoir conscience que les images et les vidéos dans lesquelles elles font l'objet d'abus sont «quelque part» et qu'elles pourraient même rencontrer quelqu'un qui a vu ce matériel est une source majeure de traumatismes et de souffrances supplémentaires.

Il semblerait que l'âge moyen des victimes d'abus sexuels d'enfants soit en constante diminution: selon la "International Association of Internet Hotlines (réseau de lignes directes INHOPE)[2], environ 70 % des victimes répertoriées dans les signalements que le réseau INHOPE a traités en 2014 se sont révélées être des enfants impubères[3]. La Internet Watch Foundation (IWF) a publié des chiffres similaires en 2015, ajoutant que 3 % des victimes semblaient avoir deux ans ou moins et qu'un tiers des images montraient des enfants violés ou subissant des tortures sexuelles[4].

1.1. Objectifs et champ d'application de l'article 25

L'objectif principal de l'article 25 de la directive[5] est d'interrompre la mise à disposition de pédopornographie[6]. Ces dispositions ont pour la première fois été introduites par la directive, car elles ne figuraient pas dans les principaux instruments législatifs en la matière, à savoir:

[1] Par exemple, The Onion Router (www.torproject.org).
[2] http://www.inhope.org/
[3] http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx
[4] https://www.iwf.org.uk/accountability/annual-reports/2015-annual-report
[5] Directive 2011/93/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie. L'article 25 de la directive concerne les «mesures contre les sites internet contenant ou diffusant de la pédopornographie».
[6] Telle que définie à l'article 2, point c), de la directive.

- la décision-cadre[7] que la directive remplace;
- la convention du Conseil de l'Europe de 2007 sur la protection des enfants contre l'exploitation et les abus sexuels, dont la directive s'inspire dans d'autres domaines; et
- la décision du Conseil relative à la lutte contre la pédopornographie sur l'Internet[8], qui a été l'un des premiers instruments juridiques au niveau de l'Union européenne concernant la pédopornographie.

L'article 25 est l'une des dispositions de la directive visant à faciliter la prévention et à atténuer la victimisation secondaire. Avec les dispositions relatives à la poursuite des crimes et à la protection des victimes, elles font partie de l'approche globale nécessaire pour lutter efficacement contre les abus sexuels des enfants, l'exploitation sexuelle des enfants et la pédopornographie.

L'article 25 dispose ce qui suit[9]:

> *1. Les États membres prennent les mesures nécessaires pour **faire rapidement supprimer** les pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire et **s'efforcent** d'obtenir la suppression des pages hébergées en dehors de celui-ci.*
>
> *2. Les États membres peuvent prendre des mesures pour **bloquer l'accès** par les internautes sur leur territoire aux pages internet contenant ou diffusant de la pédopornographie. Ces mesures doivent être établies par le biais de procédures transparentes et fournir des **garanties** suffisantes, en particulier pour veiller à ce que les restrictions soient limitées à ce qui est nécessaire et proportionnées, et que les utilisateurs soient informés de la raison de ces restrictions. Ces garanties incluent aussi la possibilité d'un recours judiciaire.*

Par conséquent, ledit article:

- impose aux États membres de **supprimer** rapidement du matériel sur les sites internet hébergés sur leur territoire;
- les oblige à **s'efforcer d'obtenir la suppression** de matériel sur des sites internet hébergés ailleurs; et
- offre la **possibilité** de **bloquer l'accès** à la pédopornographie par les internautes sur leur territoire, sous réserve d'un certain nombre de **garanties**.

Il est important de noter que l'article 25 se réfère à des «mesures», ce qui n'implique pas nécessairement des mesures législatives. Ainsi qu'il est indiqué au considérant 47 de la directive:

> *«[...] Les mesures prises par les États membres conformément à la présente directive pour supprimer ou, le cas échéant, bloquer les sites internet contenant de la pédopornographie pourraient se fonder sur diverses formes d'action publique, comme des mesures législatives, non législatives, judiciaires ou autres. Dans ce contexte, la présente directive s'entend sans préjudice des mesures*

[7] Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie.

[8] Décision 2000/375/JAI du Conseil du 29 mai 2000 relative à la lutte contre la pédopornographie sur l'Internet.

[9] Voir également les considérants 46 et 47 de la directive concernant les mesures visées à l'article 25.

volontaires adoptées par le secteur de l'internet afin de prévenir tout détournement de leurs services ou du soutien que les États membres peuvent apporter à de telles mesures. [...]»

Les mesures non législatives sont donc considérées comme transposant la directive de manière satisfaisante si elles permettent d'atteindre dans la pratique les résultats visés à l'article 25.

La coopération entre le secteur privé, y compris l'industrie et la société civile, et les autorités publiques, notamment les services répressifs et le pouvoir judiciaire, est cruciale pour mettre en œuvre les mesures prévues à l'article 25 et lutter efficacement contre la diffusion en ligne de matériel ayant trait à des abus sexuels d'enfants.

Les parties impliquées dans l'interruption de la mise à disposition en ligne de matériel ayant trait à des abus sexuels d'enfants sont:

- **les fournisseurs de services de la société de l'information (SSI)**, y compris les fournisseurs d'accès, d'hébergement et de plateformes en ligne. Dans la mesure où les criminels font une utilisation abusive des services et de l'infrastructure qu'ils fournissent, les fournisseurs de SSI sont bien placés pour coopérer à la mise en œuvre de l'article 25. Par exemple, les fournisseurs d'hébergement ont en définitive la possibilité de supprimer le matériel hébergé sur leurs serveurs et les fournisseurs d'accès, tels que les fournisseurs de services internet (FSI), peuvent bloquer l'accès;
- **les internautes**, qui pourraient tomber (de manière intentionnelle ou non) sur du matériel ayant trait à des abus sexuels d'enfants en ligne et décider de le signaler directement au fournisseur de SSI, si la technologie nécessaire est en place, par exemple par le biais d'un bouton «Signaler un abus» sur la page internet ou le navigateur. Les internautes peuvent également avoir recours à une ligne directe spéciale, gérée par une organisation de la société civile, ou au service répressif compétent;
- **des lignes directes spéciales,** généralement gérées par une ONG, une association de fournisseurs de SSI ou des entreprises de médias, qui permettent aux utilisateurs qui ne souhaitent pas s'adresser directement à la police et ne peuvent pas ou ne souhaitent pas s'adresser directement au fournisseur de SSI de faire des signalements de manière anonyme. Dans de nombreux cas, les signalements reçus dans un pays se rapportent à du matériel hébergé par des fournisseurs dans un autre pays. Sa suppression nécessite une coopération internationale, facilitée par le réseau INHOPE;
- les **services répressifs**, dont le travail s'appuie sur les signalements transmis par les lignes directes et sur ceux provenant directement des internautes. Ils échangent également des signalements en Europe (directement et par l'intermédiaire d'Europol et de son centre européen de lutte contre la cybercriminalité)[10] et au-delà (par l'intermédiaire d'Interpol)[11]; et
- le **pouvoir judiciaire**, qui veille à l'application de la loi dans chaque État membre. Dans certains pays, des décisions de justice sont nécessaires pour

[10] https://www.europol.europa.eu/ec3
[11] https://www.interpol.int/fr/Internet/Criminalité/Pédocriminalité/Pédocriminalité

supprimer ou bloquer des matériels. Eurojust[12] contribue à la coordination de la coopération judiciaire en matière pénale entre les États membres.

1.2. Objet du présent rapport et méthodologie

L'article 27 de la directive impose aux États membres[13] de mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive, et d'en transmettre le texte à la Commission au plus tard le 18 décembre 2013.

Le présent rapport répond à l'obligation prévue à l'article 28, paragraphe 2, de la directive, selon laquelle la Commission soumet au Parlement européen et au Conseil un rapport sur la mise en œuvre des mesures visées à l'article 25 de la directive[14]. Ce rapport vise à fournir un aperçu concis mais instructif des principales mesures de transposition prises par les États membres.

À la date limite de transposition, seuls 12 États membres avaient notifié à la Commission qu'ils avaient achevé la transposition de la directive. La Commission a donc ouvert des procédures d'infraction en raison de la non-communication des mesures nationales de transposition à l'encontre des autres États membres: **BE, BG, IE, EL, ES, IT, CY, LT, HU, MT, NL, PT, RO, SI** et **UK**[15]. Toutes ces procédures d'infraction avaient été clôturées au 8 décembre 2016. L'adoption et la notification tardives des mesures nationales de transposition ont retardé l'analyse et la publication par la Commission des rapports de transposition.

La description et l'analyse contenues dans le présent rapport sont fondées sur les informations communiquées par les États membres au 1er novembre 2016. Les notifications reçues après cette date n'ont pas été prises en considération. Au-delà des questions recensées dans le présent rapport, il se peut qu'il existe d'autres obstacles à la transposition, d'autres dispositions non rapportées à la Commission ou d'autres développements législatifs et non législatifs. Le présent rapport n'empêche donc pas la Commission d'évaluer ultérieurement certaines dispositions, en vue de continuer à soutenir les États membres dans la transposition et la mise en œuvre de l'article 25.

[12] http://www.eurojust.europa.eu/

[13] À partir de ce point, les termes «États membres» ou «tous les États membres» désignent les États membres liés par la directive (à savoir tous les États membres de l'Union européenne, à l'exception du Danemark). Conformément aux articles 1er et 2 du protocole 22 sur la position du Danemark, le Danemark n'a pas participé à l'adoption de la directive, et la directive ne lui est pas non plus applicable. Toutefois, la décision-cadre 2004/68/JAI du Conseil continue d'être contraignante et applicable au Danemark. Conformément à l'article 3 du protocole 21 sur la position du Royaume-Uni et de l'Irlande, les deux États membres ont pris part à l'adoption de la directive et sont liés par celle-ci.

[14] Conformément à l'article 28, paragraphe 1, de la directive, l'évaluation de la mesure dans laquelle les États membres ont pris les dispositions nécessaires pour se conformer à la directive fait l'objet d'un rapport distinct [COM(2016) 871] publié conjointement avec celui-ci.

[15] Les États-membres sont désignés dans le présent document par leur sigle, conformément aux règles suivantes: http://publications.europa.eu/code/fr/fr-370100.htm.

2. MESURES DE TRANSPOSITION

2.1. Suppression (article 25, paragraphe 1)

2.1.1. Contenu hébergé sur le territoire d'un État membre

Les États membres ont adopté deux types de mesures pour assurer la suppression rapide des pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire: des mesures fondées sur la directive 2000/31/CE[16] (directive sur le commerce électronique) et des mesures fondées sur le droit pénal national.

1. Mesures fondées sur la directive sur le commerce électronique

   La directive sur le commerce électronique définit les limitations en matière de responsabilité des prestataires intermédiaires de services internet consistant dans le simple transport, la forme de stockage dite «caching» et l'hébergement. En particulier, un fournisseur d'hébergement ne peut être tenu pour responsable si[17]:

   a. il n'a pas la connaissance ni le contrôle des informations transmises ou stockées, et

   b. dès le moment où il a effectivement connaissance ou est informé d'activités illégales, il agit promptement pour retirer les informations concernées ou rendre l'accès à celles-ci impossible.

   Ces dispositions constituent la base de l'élaboration de **procédures de notification et de retrait** des contenus illégaux. En ce qui concerne le matériel ayant trait à des abus sexuels d'enfants, ces procédures prennent la forme de mécanismes gérés par des parties intéressées visant à identifier les informations illégales hébergées sur le réseau et à faciliter leur prompte suppression.

   Les États membres ont mis en œuvre des procédures de notification et de retrait au moyen de lignes directes nationales, auxquelles les internautes peuvent signaler le matériel ayant trait à des abus sexuels d'enfants qu'ils trouvent en ligne. INHOPE est l'organisation-cadre des lignes directes. Soutenue par le programme de la Commission européenne pour un internet plus sûr[18], et depuis 2014 par le mécanisme pour l'interconnexion en Europe[19], elle représente actuellement un réseau de 51 lignes directes dans 45 pays, dont tous les États membres de l'Union.

   Les lignes directes ont signé des protocoles d'accord avec les services répressifs nationaux correspondants, qui définissent les procédures de traitement des signalements reçus des internautes. Les différentes procédures opérationnelles comportent en général les actions communes suivantes pour tout contenu hébergé dans les États membres:

   1) Détermination du lieu d'hébergement.

      Une ligne directe reçoit un signalement d'un internaute indiquant une adresse internet (URL) susceptible de contenir du matériel ayant trait à des abus sexuels d'enfants et détermine dans quel pays le matériel est hébergé. Dans certains cas,

[16] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»). Le dernier rapport de mise en œuvre a été publié en 2012: http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.
[17] Article 14 de la directive sur le commerce électronique.
[18] https://ec.europa.eu/digital-single-market/en/safer-internet-better-internet-kids
[19] https://ec.europa.eu/digital-single-market/en/connecting-europe-facility

la ligne directe reçoit le signalement d'un autre membre du réseau INHOPE, qui a déjà établi que le lieu d'hébergement était situé dans le pays de la ligne directe en question.

2) Analyse du contenu.

Si le matériel est hébergé dans le pays, la ligne directe détermine si l'adresse URL a été signalée par le passé. Si tel est le cas, le signalement est rejeté. Dans le cas contraire, la ligne directe analyse les images et les vidéos figurant à l'adresse URL et détermine si elles sont connues et si elles peuvent être illégales dans ce pays.

3) Information du fournisseur d'hébergement.

La ligne directe transmet le signalement et les analyses aux services répressifs nationaux. En fonction du protocole d'accord, le fournisseur d'hébergement est alors informé par:

- la ligne directe, après que les services répressifs ont accepté que le matériel soit supprimé, en veillant à ce que cela n'entrave pas l'enquête en cours [**AT, CZ, DE** (lignes directes eco et FSM), **FR, HU, LU, LV, NL, PL, PT, RO, SE** et **UK**]**.** Le délai entre le moment où les services répressifs sont informés par la ligne directe et le moment où cette dernière prend contact avec le fournisseur d'hébergement varie en fonction des procédures convenues entre la ligne directe et les services répressifs dans chaque État membre. Dans tous les cas, les services répressifs (se substituant ou agissant conjointement à la ligne directe) peuvent choisir d'informer le fournisseur d'hébergement, le cas échéant.
- les services répressifs, uniquement. En **BG, DE** (Jugendschutz hotline), **EE, EL, FI, MT, SI** et **SK**, les services répressifs communiquent avec le fournisseur d'hébergement, tandis que la ligne directe veille à ce que le contenu soit effectivement supprimé.

  En **CY** et **HR**, une décision de justice est requise pour exiger la suppression du matériel. Dans ces deux pays, l'accès au site internet est provisoirement bloqué jusqu'à l'adoption de la décision de justice.

Après avoir été informé de l'existence de matériel illégal sur ses serveurs, le fournisseur d'hébergement peut être tenu responsable s'il ne le supprime pas conformément aux lois nationales de transposition. La seule limite à l'imputation de responsabilité est l'exemption de responsabilité prévue par la directive sur le commerce électronique telle que mise en œuvre par les États membres (voir ci-dessus).

Au moment de la rédaction du présent rapport, la plupart des États membres disposaient de lignes directes capables d'évaluer le contenu signalé pour mettre en œuvre des procédures de notification et de retrait, à l'exception de **BE, ES** et **IT**:

- **BE** a signalé avoir récemment adopté une loi qui permet à une ligne directe INHOPE d'opérer dans le pays et de traiter les signalements selon la procédure générale décrite ci-dessus. Au moment de la rédaction du présent rapport, la police et le pouvoir judiciaire belges négociaient avec la ligne directe un protocole d'accord et des protocoles opérationnels.
- La situation en **ES** nécessite un examen plus approfondi en ce qui concerne la situation de la ligne directe.

- **IT** dispose de deux lignes directes INHOPE, mais la législation actuelle ne leur permet pas de vérifier le contenu des signalements reçus d'internautes ou d'autres lignes directes. Par conséquent, elles se contentent de transmettre les signalements aux services répressifs (centre national de lutte contre la pédopornographie en ligne, CNCPO), sans en vérifier le contenu.

2. Mesures fondées sur le droit pénal national

Les États membres ont notifié deux types de dispositions pénales qui permettent également la suppression des contenus illégaux hébergés sur leur territoire:

a. des dispositions générales qui permettent la saisie de matériels relevant d'une procédure pénale, par exemple le matériel utilisé lors de la commission d'une infraction: **AT, CZ, HU, IT, LU, NL, SE** et **SK**; et

b. des dispositions spécifiques relatives à la suppression de matériel pédopornographique: **CY, EE, EL, ES, SE** et **UK** (**Gibraltar**).

La législation de **CZ**, **EL**, **HU** et **UK (Gibraltar)** fait explicitement référence à l'exigence d'une suppression rapide: «sans délai indu» (**CZ**), «exécuté immédiatement» (**EL**), «dans les 12 heures» (**HU**) ou «suppression rapide» [**UK (Gibraltar)**].

D'autres États membres transposent cette exigence au moyen des procédures de notification et de retrait décrites ci-dessus, les voies de droit pénal pouvant alors n'être utilisées que de manière accessoire pour faire face aux difficultés rencontrées dans la mise en œuvre des mécanismes de notification et de retrait (par exemple, en cas de non coopération du fournisseur d'hébergement) ou lorsque le matériel est lié à une enquête criminelle en cours. Dans les États membres qui ne disposent pas de mécanismes de notification et de retrait fonctionnels ou lorsque le droit pénal ne prévoit pas la suppression rapide, il est nécessaire d'obtenir davantage d'informations sur les mesures prises pour transposer cette exigence.

2.1.2. Contenu hébergé en dehors du territoire d'un État membre

Tous les États membres, à l'exception de **BE, ES** et **IT**, ont transposé cette disposition au moyen d'une ligne directe pleinement opérationnelle (c'est-à-dire autorisée à évaluer le matériel) et de la procédure suivante visant à supprimer le contenu hébergé hors de leur territoire:

1) après avoir constaté que le lieu d'hébergement se trouve en dehors de l'État membre, les opérateurs de la ligne directe qui a reçu le signalement vérifient s'il existe une ligne directe INHOPE opérationnelle dans le pays d'hébergement;

2) si le pays d'hébergement dispose d'une ligne directe INHOPE, le signalement lui est envoyé par l'intermédiaire du système interne d'échange d'informations INHOPE, afin qu'elle puisse traiter le signalement selon la procédure nationale applicable au contenu hébergé dans le pays;

3) si le pays d'accueil ne dispose pas d'une ligne directe INHOPE, le signalement est envoyé aux services répressifs du pays où il a été reçu, qui le transmet, généralement via Europol ou Interpol, aux services répressifs du pays d'hébergement.

Bien que les procédures appliquées par les différentes lignes directes suivent en général un modèle similaire, il existe certaines spécificités, en fonction de ce qui a été convenu entre la ligne directe et les services répressifs. Par exemple, certaines lignes directes (notamment en **DE, LT** et **LV**) adressent une notification au fournisseur d'hébergement à l'étranger si aucune mesure n'a été prise après un certain temps. Certaines lignes directes (par exemple en **AT, CZ, DE, FR, LU, MT**) informent les services répressifs de leur

pays lorsqu'elles transmettent un signalement à une ligne directe à l'étranger, alors que d'autres (par exemple **HU**, **NL, PL, SE** et **UK**) ne le font généralement pas. Enfin, si le pays d'hébergement n'est doté d'aucune ligne directe INHOPE, certaines lignes directes (par exemple, en **EE, LU** et **UK**) prennent contact, le cas échéant, avec des lignes directes non affiliées au réseau INHOPE.

Les États membres qui ne disposent pas d'une ligne directe pleinement opérationnelle (**BE, ES** et **IT**) transposent cette disposition en assurant l'échange d'informations, généralement via Europol ou Interpol, entre les services répressifs du pays d'origine du signalement et ceux du pays dans lequel le matériel est hébergé. Dans ce cas, des informations supplémentaires relatives à la transposition de la disposition par ce mécanisme sont nécessaires, notamment en ce qui concerne les cas où les pages internet hébergées à l'étranger ne sont liées à aucune procédure pénale dans cet État membre et ne font l'objet d'aucune demande d'entraide judiciaire.

En ce qui concerne la rapidité et l'efficacité de la suppression au moyen des lignes directes, d'après les données fournies par celles-ci, 93 % du matériel ayant trait à des abus sexuels d'enfants traité par les lignes directes en Europe et 91 % du matériel traité par les lignes directes dans le monde ont été supprimés en moins de 72 heures[20].

2.2. Blocage (article 25, paragraphe 2)

Environ la moitié des États membres (**BG, CY, CZ, EL, ES, FI, FR, HU, IE, IT, MT, PT, SE** et **UK**) ont choisi d'appliquer des mesures facultatives de blocage au titre de l'article 25, paragraphe 2. La diversité des mesures reflète le libellé du considérant 47 de la directive (mesures législatives, non législatives, judiciaires ou autres, notamment les mesures volontaires adoptées par le secteur de l'internet).

On peut classer les mesures selon qu'une décision de justice est nécessaire ou non pour bloquer un site internet. Une décision de justice est:

- requise en **EL, ES** et **HU**;
- facultative
    - en **CY, FR, IT** et **PT**, où les FSI sont tenus par la loi de se conformer à la demande formulée par les autorités (c'est-à-dire les services répressifs ou l'autorité de régulation nationale) de bloquer le site; et
    - en **BG, CZ, IE, FI, MT, SE** et **UK**, où les FSI ne sont pas expressément tenus par la loi de se conformer à la demande des autorités, mais le font volontairement.

Des listes noires de sites internet contenant ou diffusant de la pédopornographie sont couramment utilisées dans la mise en œuvre de mesures de blocage. Ces listes noires sont généralement préparées par les autorités nationales (c'est-à-dire les services répressifs ou l'autorité de régulation) et transmises aux FSI. Certains États membres (**EL, HU, IT, FI** et **FR**) ont notifié une législation régissant ce processus.

BG utilise la liste des «pires sites» («Worst of List») d'Interpol[21], alors que **UK** utilise la liste d'adresses URL de l'IWF[22]. Les FSI en **CZ** utilisent également la liste de l'IWF sur une base d'autorégulation.

[20]http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx

[21]https://www.interpol.int/fr/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list

De manière générale, les informations reçues des États membres n'étaient pas concluantes en ce qui concerne le nombre de pages internet contenues dans les listes de blocage ou le nombre de tentatives bloquées.

La directive exige que les mesures prises pour bloquer l'accès aux sites internet contenant ou diffusant de la pédopornographie prévoient des procédures transparentes et des garanties suffisantes. Le considérant 47 indique ce qui suit:

> *Quelle que soit la base retenue pour agir ou la méthode choisie, les États membres devraient veiller à ce qu'elles assurent aux utilisateurs et aux fournisseurs d'accès un degré suffisant de sécurité juridique et de prédictibilité. En vue aussi bien de retirer que de bloquer des contenus pédopornographiques, il convient de favoriser et de renforcer la coopération entre les autorités publiques, en particulier afin de garantir, dans la mesure du possible, l'exhaustivité des listes nationales énumérant les sites internet contenant du matériel pédopornographique et d'éviter tout double emploi. Toute évolution de ce type doit tenir compte des droits de l'utilisateur final et être conforme aux procédures juridiques et judiciaires existantes, ainsi qu'à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et à la charte des droits fondamentaux de l'Union européenne.*

Plus précisément, l'article 25, paragraphe 2, fait référence aux exigences suivantes:

1. des procédures transparentes;
2. la limitation à ce qui est nécessaire et proportionné;
3. l'information des utilisateurs sur les raisons de la restriction; et
4. la possibilité d'un recours judiciaire.

Les États membres qui ont opté pour la transposition de cette disposition ont intégré une série de procédures transparentes et de garanties:

- en **EL**, la commission hellénique des télécommunications et postes notifie les décisions des autorités compétentes aux fournisseurs de services internet et exige le blocage immédiat du contenu et la communication d'informations pertinentes aux utilisateurs. Le propriétaire de la page internet peut former un recours contre la décision dans un délai de deux mois;

- en **ES**, au cours de la procédure pénale, le juge peut ordonner la fermeture d'un site internet contenant de la pédopornographie à titre de mesure de précaution, qui peut être contestée. Le prestataire de services est tenu de fournir les informations nécessaires aux clients;

- en **FI**, la police peut établir, tenir et mettre à jour une liste de sites de pédopornographie. Lorsqu'un site est bloqué, la police doit publier une déclaration indiquant les raisons du blocage, qui doit s'afficher chaque fois que l'accès à un site est bloqué. Les recours contre les décisions de la police qui visent à ajouter un site à la liste de blocage peuvent être introduits devant un tribunal administratif;

- en **FR**, les fournisseurs d'accès internet doivent bloquer l'accès aux adresses internet concernées dans un délai de 24 heures. La liste des sites internet est examinée par une personne qualifiée de la commission nationale de l'informatique et des libertés. Les utilisateurs qui tentent d'accéder à un service auquel l'accès leur est refusé sont redirigés vers une adresse informative du

[22] https://www.iwf.org.uk/members/member-policies/url-list/blocking-faqs#WhatistheIWFURLlist

ministère de l'intérieur, indiquant les raisons du refus d'accès et les procédures de recours disponibles devant le tribunal administratif;

- en **HU**, l'accès peut être bloqué de manière provisoire ou permanente. Les demandes sont reçues par le ministre de la justice et, le cas échéant, soumises à la cour métropolitaine de Budapest. L'obligation de bloquer l'accès incombe au FSI qui fournit la connectivité. La transparence de la procédure est assurée puisque la décision de la cour est notifiée par voie de publication et est donc accessible au public. Il est possible d'interjeter appel contre une ordonnance de blocage permanent;
- en **IT**, le centre national de lutte contre la pédopornographie sur l'internet fournit aux FSI une liste de sites de pédopornographie, auxquels ils empêchent l'accès à l'aide d'outils de filtrage et de technologies connexes. Les sites auxquels l'accès est bloqué afficheront une «page de blocage» indiquant les raisons du blocage; et
- en **UK** (**Angleterre/Pays de Galles**, **Irlande du Nord** et **Écosse**), des mesures visant à bloquer l'accès à ces pages internet sont prises par l'intermédiaire de l'IWF, organisme privé d'autorégulation qui formule des recommandations de blocage ou de filtrage de contenu. Une procédure d'appel permet à toute personne légitimement associée au contenu en question, ou qui y a un intérêt légitime, de contester l'exactitude de l'évaluation. En **UK** (**Gibraltar**), l'autorité de régulation de Gibraltar peut, de concert avec les FSI, bloquer l'accès aux pages internet qui contiennent ou diffusent de la pédopornographie auprès des utilisateurs de Gibraltar. Ces mesures doivent être transparentes, limitées à ce qui est strictement nécessaire, proportionnées et motivées.

En **BG, CY, CZ, IE, MT, PT** et **SE**, les informations fournies sur les garanties applicables aux mesures de blocage n'étaient pas concluantes et nécessiteront un examen plus approfondi.

3. CONCLUSIONS ET ÉTAPES SUIVANTES

La Commission reconnaît les efforts importants déployés par les États membres pour transposer l'article 25 de la directive.

Toutefois, des améliorations doivent encore être apportées afin d'utiliser pleinement son potentiel en continuant de travailler à sa mise en œuvre complète et appropriée dans tous les États membres. Parmi les principaux défis à relever, il convient de veiller à ce que le matériel ayant trait à des abus sexuels d'enfants sur le territoire des États membres soit rapidement supprimé et à ce que des garanties suffisantes soient fournies lorsque l'État membre choisit de prendre des mesures pour bloquer l'accès par les internautes sur son territoire à des pages internet contenant du matériel ayant trait à des abus sexuels d'enfants.

Par conséquent, la Commission n'a pas l'intention, pour l'heure, de proposer des modifications de l'article 25 ou une législation complémentaire. Elle veillera plutôt surtout à ce que les enfants bénéficient de la pleine valeur ajoutée de l'article, grâce à sa transposition et à sa mise en œuvre complètes par les États membres.
Cela étant dit, la Commission a souligné dans sa récente communication sur les plateformes en ligne[23] la nécessité de soutenir et de développer des processus d'engagement multipartites destinés à trouver des solutions communes pour déceler et lutter résolument contre le matériel illicite en ligne et s'est engagée à examiner la nécessité de procédures officielles de notification et d'action.

La Commission continuera à fournir un soutien aux États membres pour assurer un niveau de transposition et de mise en œuvre satisfaisant. Cela implique notamment de s'assurer que les mesures nationales sont conformes aux dispositions correspondantes de l'article et de faciliter l'échange des meilleures pratiques. Le cas échéant, la Commission fera usage de ses pouvoirs d'exécution en vertu des traités au moyen de procédures d'infraction.

[23] Communication intitulée «Les plateformes en ligne et le marché unique numérique - Perspectives et défis pour l'Europe» [COM(2016) 288], du 25 mai 2016.