EUROPEAN
COMMISSION

Brussels, 16.12.2016
COM(2016) 872 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography

Contents

1. INTRODUCTION 3
1.1. Objectives and scope of Article 25 3
1.2. Purpose of this report and methodology 5
2. TRANSPOSITION MEASURES 7
2.1. Removal (Article 25(1)) 7
2.1.1. Content hosted in a Member State's territory 7
2.1.2. Content hosted outside a Member State's territory 9
2.2. Blocking (Article 25(2)) 10
3. CONCLUSION AND NEXT STEPS 12

1. INTRODUCTION

The Internet has brought about a dramatic increase in child sexual abuse in that:

- it facilitates the sharing of child sexual abuse material, by offering a variety of distribution channels such as the web, peer-to-peer networks, social media, bulletin boards, newsgroups, Internet relay chats and photo-sharing platforms, among many others. Sharing is also facilitated by access to a worldwide community of like-minded individuals, which is a source of strong demand and mutual support;
- it provides technical means and security measures that can facilitate anonymity;[1]
- as a consequence of the strong demand for child sexual abuse material, children continue to be at risk of becoming victims, while anonymity can obstruct the investigation and prosecution of these crimes; and
- new child sexual abuse materials have become a currency. To obtain and maintain access to forums, participants frequently have to submit new materials on a regular basis, which encourages the commission of child sexual abuse.

Online child sexual abuse is a nefarious crime with long-term consequences for its victims. Harm is caused not only when the abuse is actually recorded or photographed, but also every time the images and videos are posted, circulated and viewed. For the victims, the realisation that the images and videos in which they are abused are 'out there' and that they could even encounter someone who has seen the material is a major source of trauma and additional suffering.

There are indications that the average age of victims of child sexual abuse material is steadily decreasing: according to the International Association of Internet Hotlines (INHOPE),[2] around 70% of the victims in the reports that INHOPE hotlines processed in 2014 appeared to be prepubescent.[3] The Internet Watch Foundation (IWF) issued similar figures in 2015, adding that 3% of the victims appeared to be two years old or younger and a third of images showed children being raped or sexually tortured.[4]

1.1. Objectives and scope of Article 25

The main objective of Article 25 of the Directive[5] is to disrupt the availability of child pornography.[6] Such provisions were first introduced with the Directive, as they were not included in the main legislative instruments in the area, i.e.:

- the Framework Decision[7] that the Directive replaces;
- the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, from which the Directive draws inspiration in other areas; or

[1] e.g. 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/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. Article 25 of the Directive covers 'measures against websites containing or disseminating child pornography'.
[6] As defined in Article 2(c) of the Directive.
[7] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

- the Council Decision to combat child pornography on the Internet,[8] which was one of the first legal instruments at EU level that addressed child pornography.

Article 25 is one of a number of provisions in the Directive to facilitate prevention and mitigate secondary victimisation. Together with provisions on the prosecution of crimes and protection of victims, they are part of the holistic approach required to tackle child sexual abuse, child sexual exploitation and child pornography effectively.

Article 25 reads as follows:[9]

> *1. Member States shall take the necessary measures to **ensure the prompt removal** of web pages containing or disseminating child pornography hosted in their territory and to **endeavour** to obtain the removal of such pages hosted outside of their territory.*
>
> *2. Member States may take measures to **block access** to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate **safeguards**, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.*

It therefore:

- obliges Member States to **remove** promptly material on websites hosted within their territory;
- obliges them to **endeavour to secure the removal** of material on websites hosted elsewhere; and
- offers the **possibility** to **block access** to child pornography by users within their territory, subject to a number of **safeguards**.

It is important to note that Article 25 refers to 'measures', which may not necessarily involve legislation. As recital 47 of the Directive states:

> *"… The measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other. In that context, this Directive is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States…"*

Non-legislative measures are therefore considered to transpose the Directive satisfactorily if they allow the outcomes specified in Article 25 to be achieved in practice.

Cooperation between the private sector, including industry and civil society, and public authorities, including law enforcement agencies (LEAs) and the judiciary, is crucial to implementing the measures under Article 25 and effectively fighting the dissemination of child sexual abuse material online.

[8] Council Decision 2000/375/JHA of 29 May 2000 to combat child pornography on the Internet.
[9] See also recitals 46 and 47 of the Directive concerning the measures referred to in Article 25.

The parties involved in disrupting the availability of child sexual abuse material online are:

- **information society service providers (ISSPs)**, including providers of access, hosting and online platforms. As criminals abuse the services and the infrastructure they provide, ISSPs are well placed to cooperate in the implementation of Article 25. For example, hosting providers are ultimately able to remove material hosted on their servers and access providers such as internet service providers (ISPs) can block access;
- **Internet users,** who may come across child sexual abuse material online (intentionally or unintentionally) and decide to report it to the ISSP directly if the technology to do so is in place, e.g. through a 'report abuse' button on the web page or browser. Users may also report to a dedicated hotline run by a civil society organisation, or to the LEA responsible;
- **dedicated hotlines,** usually run by an NGO or an association of ISSPs or media companies, which allow anonymous reporting by users who may not feel comfortable reporting to the police and cannot or do not wish to report to the ISSP directly. In many cases, reports received in one country refer to material hosted by providers in another. Its removal requires international cooperation, which INHOPE facilitates;
- **LEAs**, whose work is supported by reports passed on by hotlines and directly from Internet users. They also share reports with each other in Europe (directly and through Europol and its European Cybercrime Centre)[10] and beyond (through Interpol);[11] and
- the **judiciary**, which ensures application of the law in each Member State. In some countries, court orders are needed to remove or block material. Eurojust[12] helps coordinate judicial cooperation in criminal matters across Member States.

1.2. Purpose of this report and methodology

Article 27 of the Directive requires Member States[13] to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive and communicate them to the Commission by 18 December 2013.

This report responds to the requirement under Article 28(2) of the Directive for the Commission to submit a report to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of the Directive.[14] The report aims to provide a concise yet informative overview of the main transposition measures taken by Member States.

[10] https://www.europol.europa.eu/ec3
[11] http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children
[12] http://www.eurojust.europa.eu/
[13] From this point onwards, 'Member States' or 'all Member States' refer to the Member States bound by the Directive (i.e. all EU Member States except Denmark). In accordance with Articles 1 and 2 of Protocol 22 on the Position of Denmark, Denmark did not take part in the adoption of the Directive, nor does the Directive apply to it. However Council Framework Decision 2004/68/JHA continues to be applicable to and binding upon Denmark. In accordance with Article 3 of Protocol 21 on the position of the United Kingdom and Ireland, both took part in the adoption of the Directive and are bound by it.
[14] In accordance with Article 28(1) of the Directive, the extent to which the Member States have taken the necessary measures to comply with the Directive is assessed in a separate report (COM(2016) 871) published jointly with this one.

By the transposition deadline, only 12 Member States had notified the Commission that they had completed transposition of the Directive. The Commission therefore opened infringement proceedings for non-communication of national transposition measures against the others: **BE, BG, IE, EL, ES, IT, CY, LT, HU, MT, NL, PT, RO, SI** and the **UK**.[15] All these infringement proceedings had been closed by 8 December 2016. The late adoption and notification of national transposition measures delayed the Commission's analysis and publication of the transposition reports.

The description and analysis in this report are based on the information that Member States provided by 1 November 2016. Notifications received after that date have not been taken into account. Beyond the issues identified in this report, there may be both further challenges in transposition and other provisions not reported to the Commission or further legislative and non-legislative developments. Therefore, this report does not prevent the Commission from further evaluating some provisions, to continue supporting Member States in the transposition and implementation of Article 25.

[15] Member States in this document are abbreviated according to these rules: http://publications.europa.eu/code/en/en-370100.htm

2. TRANSPOSITION MEASURES

2.1. Removal (Article 25(1))

2.1.1. Content hosted in a Member State's territory

Member States have adopted two types of measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in a Member State's territory: measures based on Directive 2000/31/EC[16] (E-commerce Directive), and measures based on national criminal law.

1. Measures based on the E-commerce Directive

   The E-commerce Directive defines the liability limitations of an Internet intermediary providing services consisting of mere conduit, caching and hosting. In particular, a hosting provider cannot be held liable if:[17]

   a. it has neither knowledge of nor control over the information that is transmitted or stored, and

   b. upon obtaining actual knowledge or awareness of illegal activities, it acts expeditiously to remove or to disable access to the information concerned.

   These provisions constitute the basis for the development of **notice and take down procedures** for illegal content. In the area of child sexual abuse material, these procedures take the form of mechanisms run by interested parties aimed at identifying illegal information hosted on the network and at facilitating its rapid removal.

   Member States have implemented notice and take down procedures through national hotlines, to which Internet users can report child sexual abuse material that they find online. INHOPE is the umbrella organisation for the hotlines. Supported by the European Commission's Safer Internet Programme[18], and since 2014 by the Connecting Europe Facility framework,[19] it currently represents a network of 51 hotlines in 45 countries, including all EU Member States.

   The hotlines have memoranda of understanding with the corresponding national LEAs, which set out procedures for handling the reports received from Internet users. The different operating procedures include in general the following common actions for content hosted in the Member States:

   1) Determine the hosting location.

      A hotline receives an Internet user's report of a web address (URL) with possible child sexual abuse material and determines in which country the material is hosted. In some cases, the hotline receives the report from another INHOPE network member, which has already determined that the hosting location is in the country of the hotline in question.

[16] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). The last implementation report was published in 2012: http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf

[17] Article 14 of E-commerce Directive.

[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

2) Analyse content.

If the material is hosted in the country, the hotline determines whether the URL has been reported previously. If so, the report is discarded. Otherwise, the hotline analyses the images and videos on the URL and determines whether they are known and whether they may be illegal in that country.

3) Inform hosting provider.

The hotline forwards the report and the analyses to the national LEA. Depending on the memorandum of understanding, the hosting provider is then informed by:

- the hotline, after the LEA has agreed that the material can be taken down, ensuring that this would not interfere with an ongoing investigation (**AT, CZ, DE** (eco and FSM hotlines), **FR, HU, LU, LV, NL, PL, PT, RO, SE** and the **UK).** The time between the hotline first informing the LEA and the hotline communicating with the hosting provider varies depending on the procedures agreed between the hotline and the LEA in each Member State. In any case, the LEA (instead of or in addition to the hotline) may choose to inform the hosting provider as circumstances require.
- the LEA only. In **BG, DE** (Jugendschutz hotline), **EE, EL, FI, MT, SI** and **SK**, the LEA communicates with the hosting provider, while the hotline monitors that the content is actually removed.

  In **CY** and **HR,** a court order is required to request the removal of the material. In both countries, access to the website is temporarily blocked until the court order is obtained.

After being made aware of the existence of illegal material on its servers, the hosting provider can be held liable if it fails to remove it in accordance with the national implementing laws. The only limit to the attribution of liability is the liability exemption under the E-commerce Directive as implemented by Member States (see above).

At the time of writing, most Member States have hotlines that are capable of assessing reported content to implement notice and take down procedures, except **BE, ES** and **IT:**

- **BE** notified recently adopted legislation that allows an INHOPE hotline to operate in the country and handle reports according to the general procedure described above. At the time of writing, the Belgian police and judiciary were negotiating with the hotline a memorandum of understanding and the operating protocols.
- The situation in **ES** requires closer examination with regard to the hotline situation.
- **IT** has two INHOPE hotlines, but the current legislation does not allow them to check the content of reports received from Internet users or other hotlines. Therefore, they simply forward the reports to the LEA (the National Centre for Combatting Online Child Pornography, CNCPO), without checking the content.

2. Measures based on national criminal law

Member States have notified two types of criminal law provisions which also allow the removal of illegal content hosted in their territory:

a. general provisions that allow the seizure of material relevant to criminal proceedings, e.g. material used in the commission of an offence: **AT, CZ, HU, IT, LU, NL, SE** and **SK**; and

b. specific provisions on the removal of child pornography: **CY, EE, EL, ES, SE,** and **UK (Gibraltar)**.

The legislation in **CZ**, **EL**, **HU** and **UK (Gibraltar)** makes explicit reference to the requirement of prompt removal: 'without undue delay' (**CZ**), 'executed immediately' (**EL**), 'within 12 hours' (**HU**) or 'prompt removal' (**UK (Gibraltar)**).

Other Member States transpose this requirement through the notice and takedown procedures described above, which may lead to the criminal law channels being used only in an ancillary way to deal with cases where notice and takedown mechanisms encounter difficulties (e.g. for lack of cooperation of the hosting provider) or where material is linked to an ongoing criminal investigation. In Member States without functional notice and take down mechanisms or where criminal law does not specify prompt removal, more information is needed on the measures taken to transpose this requirement.

2.1.2. Content hosted outside a Member State's territory

All Member States except **BE, ES** and **IT** have transposed this provision through a fully operational hotline (i.e. a hotline authorised to assess the material) and the following operating procedure to endeavour to remove content hosted outside their territory:

1) once the operators of the hotline that has received the report determine that the hosting location is outside of the Member State, they verify whether there is an operational INHOPE hotline in the hosting country;

2) if the hosting country has an INHOPE hotline, the report is sent to it through the internal INHOPE information exchange system, so that it can process the report according to the national procedure for content hosted in the country;

3) if the hosting country does not have an INHOPE hotline, the report is sent to the LEA of the country in which it was received, which forwards it, usually via Europol or Interpol, to the LEA of the hosting country.

Although the procedures across hotlines follow in general a similar pattern, there are some specificities depending on what has been agreed between the hotline and the LEA. For example, some hotlines (e.g. in **DE, LT** and **LV**) notify the hosting provider abroad if no action has been taken after a certain time. Some hotlines (e.g. in **AT, CZ, DE, FR, LU, MT**) inform the LEA of their country when they forward a report to a hotline abroad, while others (e.g. in **HU**, **NL, PL, SE** and the **UK**) generally do not. Finally, if there is no INHOPE hotline in the hosting country, some hotlines (e.g. in **EE, LU,** and the **UK**) contact non-INHOPE hotlines there, if they exist.

Member States without a fully operational hotline (**BE, ES** and **IT**) transpose this provision by arranging for the exchange of information, usually via Europol or Interpol, between the LEA in the country in which the report originated and that of the country in which the material is hosted. In this case, more information is needed on the transposition of the provision through this mechanism, in particular in relation to cases where the web pages hosted abroad are not linked to any criminal proceedings in that Member State and are not the object of any request for mutual legal assistance (MLA).

With regard to the promptness and effectiveness of removal through the hotlines, according to their data, 93% of the child sexual abuse material processed by the hotlines

in Europe and 91% of the material processed by the hotlines worldwide was removed from Internet public access in less than 72 hours.[20]

2.2. Blocking (Article 25(2))

About half of the Member States (**BG, CY, CZ, EL, ES, FI, FR, HU, IE, IT, MT, PT, SE** and the **UK**) have chosen to apply optional blocking measures under Article 25(2). The variety of the measures reflects the wording of recital 47 of the Directive (legislative, non-legislative, judicial or other, including voluntary action by the Internet industry).

One way to classify the measures is according to whether a court order is required to block a website. A court order is:

- required in **EL, ES** and **HU**;
- not mandatory in
    - **CY, FR, IT** and **PT**, where ISPs are required by law to comply with the request of the authorities (i.e. the LEA or the national regulator) to block the site; and
    - **BG, CZ, IE, FI, MT, SE,** and the **UK**, where ISPs are not explicitly required by law to comply with the authorities' request but do so voluntarily.

Blacklists of websites containing or disseminating child pornography are commonly used in the implementation of blocking measures. Blacklists are typically prepared by national authorities (i.e. the LEA or the regulator) and transmitted to the ISPs. Some Member States (**EL, HU, IT, FI** and **FR**) notified legislation that governs this process.

BG uses Interpol's 'Worst of List',[21] while the **UK** uses IWF's URL list.[22] ISPs in **CZ** also use the IWF list on a self-regulatory basis.

Information received from Member States was, in general, not conclusive as to the number of webpages included in blocking lists, or the number of attempts blocked.

The Directive requires that measures taken to block access to websites containing or disseminating child pornography provide for transparent procedures and adequate safeguards. Recital 47 states that:

> *Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability to users and service providers. Both with a view to the removal and the blocking of child abuse content, cooperation between public authorities should be established and strengthened, particularly in the interests of ensuring that national lists of websites containing child pornography material are as complete as possible and of avoiding duplication of work. Any such developments must take account of the rights of the end users and comply with existing legal and judicial procedures and the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union.*

Specifically, Article 25(2) refers to the following requirements:

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

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

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

1. transparent procedures;
2. limitation to what is necessary and proportionate;
3. information to users on the reasons for restriction; and
4. possibility of judicial redress.

Member States which opted to transpose this provision have done so incorporating a variety of transparent procedures and safeguards:

- in **EL,** the Hellenic Telecommunication and Post Commission notifies orders of the competent authorities to providers of Internet access services and urges immediate content blocking and the provision of relevant information to users. The owner of the webpage may appeal against the order within a period of two months;
- in **ES**, during the criminal proceedings, the judge may order the closure of a website containing child pornography as a precautionary measure, which can be contested. The service provider is obliged to provide the necessary information to customers;
- in **FI**, the police may establish, maintain and update a list of child pornography sites. Where a website is blocked, the police have to issue a statement giving the reasons for the blocking which must be displayed every time access to a site is blocked. Appeals against decisions by the police to add a site to the blocking list can be lodged with an administrative court;
- in **FR**, Internet providers must block access to the Internet addresses concerned within 24 hours. The list of websites is reviewed by a qualified person from the National Commission on Computing and Freedoms. Users trying to reach the service to which access is denied are redirected to an information address of the Ministry of Interior, stating the reasons for denial of access and the available redress procedures before the administrative court;
- in **HU**, access can be blocked temporarily or permanently. Requests are received by the Minister of Justice and, where appropriate, submitted to the Metropolitan Court of Budapest. The obligation to block access rests with the ISP providing connectivity. The transparency of the procedure is ensured as the decision of the court is served by way of publication and is thus accessible to the public. Judicial appeal is available against an order of permanent blocking;
- in **IT**, the National Centre for Combating Child Pornography on the Internet provides ISPs with a list of child pornography sites, to which they prevent access using filtering tools and related technology. The sites to which access is blocked will display a 'stop page' indicating the reasons for blocking; and
- in the **UK** (**England**/**Wales**, **Northern Ireland** and **Scotland**), measures to block access to such webpages are taken through IWF, which works as a private self-regulatory body that makes recommendations to have content blocked or filtered. There is an appeals process whereby anyone with a legitimate association with or interest in the content in question can contest the accuracy of the assessment. In the **UK** (**Gibraltar**), the Gibraltar Regulatory Authority may, in conjunction with IPSs, block access to web pages that contain or disseminate child pornography to users in Gibraltar. Such measures must be transparent, limited to what is strictly necessary, proportionate and reasoned.

In **BG, CY, CZ, IE, MT, PT** and **SE** the information provided on safeguards applicable to blocking measures was not conclusive and will require further examination.

3. CONCLUSION AND NEXT STEPS

The Commission acknowledges the significant efforts made by the Member States in the transposition of Article 25 of the Directive.

There is still room, however, to use its potential to the full by continuing to work on its complete and correct implementation across Member States. Some key challenges ahead include ensuring that child sexual abuse material in Member States' territory is removed promptly and that adequate safeguards are provided where the Member State opts to take measures to block access to Internet users within its territory to web pages containing child sexual abuse material.

Therefore, for the time being, the Commission has no plans to propose amendments to Article 25 or complementary legislation. It will instead focus its efforts on ensuring that children benefit from the full added value of the Article, through its complete transposition and implementation by Member States.
That said, in its recent Communication on Online Platforms,[23] the Commission highlighted the need to sustain and develop multi-stakeholder engagement processes aimed at finding common solutions to voluntarily detect and fight illegal material online and committed to reviewing the need for formal notice and action procedures.

The Commission will continue to provide support to Member States to ensure a satisfactory level of transposition and implementation. This includes monitoring that national measures comply with the corresponding provisions in the Article and facilitating the exchange of best practices. Where necessary, the Commission will make use of its enforcement powers under the Treaties through infringement procedures.

[23] Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM/2016/288), of 25 May 2016.