

EDRi's position paper on the European Commission's implementation report on Article 25 of Directive 2011/92/EU

European Digital Rights (EDRi) is an association of [civil and human rights organisations](#) from across Europe. We defend rights and freedoms in the digital environment.

EDRi followed closely and worked constructively in the legislative process that led to Directive 2011/92/EU. In view of the [European Commission's report](#) assessing the implementation of the measures referred to in Article 25 of the [Directive 2011/92/EU](#) of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (hereafter referred to as "the report"), EDRi takes the opportunity to comment on it and make recommendations.

Introduction

The report describes the purpose of Article 25 of Directive 2011/92/EU as being the "disruption of the availability" of "child pornography" and describes the obligations on Member States to achieve this goal as:

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

On the last of these points, the Commission's report incorrectly says that Recital 47 permits the use of non-legislative means to "allow the outcomes specified in Article 25 to be achieved in practice". **This is not legally correct, as this would mean that the safeguards contained in Article 25 (which are not "outcomes" *per se*) could be ignored if voluntary arrangements were used.** This is the same as the legal analysis contained in a [letter](#) that EDRi received from the Commission on 26 November 2012 in response to [our concerns](#) on this issue. This analysis is not in line with the obligations set forth in Articles 51 and 52 of the Charter of Fundamental Rights of the European Union.

The Commission then lists the following parties as being "crucial to implementing the measures in Article 25":

- industry
- civil society
- public authorities, including law enforcement agencies (LEAs) and the judiciary

Notice and takedown

In relation to reports being made to the hosting service by a hotline, the report states that "[t]he 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".

The report fails to address and analyse how quickly or slowly that might be happening, nor the average, nor anything about the nature of the procedures that have been agreed.

- No statistics are provided regarding the speed of removal of content, except for two figures on removals in 72 hours or less.
- No statistics are provided regarding the frequency with which reports are followed up by law enforcement authorities.
- No statistics are provided regarding delays in takedowns due to the need to avoid interference with ongoing investigations.
- No data is provided with regard to nationally-agreed procedures for expedited storage of evidence in relation to sites that have been taken down.
- No statistics are provided with regard to the frequency with which any such stored data are actually used by judicial or law enforcement authorities.
- No information is given regarding procedures for processing reports (such as security of information transfer between the three “crucial” stakeholders – industry, civil society and public authorities).

Measures based on criminal law

No statistics are provided with regard to use of criminal law procedures to seize equipment in relevant cases.

The report states, without further explanation that “more information is needed” from Member States where there is neither functional notice and take-down (nor how this can be the case 16 years after the implementation of the E-Commerce Directive) nor criminal measures in place.

Content hosted outside a Member State’s territory

There appears to have been no verification of whether the INHOPE system correctly and speedily transfers reports to counterparts in third countries. The report appears to simply assume that this is happening and that no improvements are possible.

The acknowledgement that “some hotlines (e.g. in DE, LT and LV) notify the hosting provider abroad if no action has been taken after a certain time” based on apparently *ad hoc* arrangements with national law enforcement authorities is worrying, but no further explanation is given. It is entirely unacceptable that the Commission can acknowledge that Member State law enforcement authorities are not respecting national obligations under the Directive without explaining how often this is happening, in which countries this is happening and what the European Commission is planning to do in order to ensure that the provisions of the Directive are respected. Insofar as similar situations can be envisaged with regard to third countries, this, too, is not examined.

Having described “public authorities, including law enforcement agencies (LEAs) and the judiciary” as “crucial to implementing the measures in Article 25”, many of the procedures listed in section 2.1.2 of the Commission’s report involve no public authorities at all.

Again, no statistics regarding any of the scenarios described were provided. In addition, no statistics are provided with regard to data requested under Mutual Legal Assistance for data hosted abroad.

The Commission blandly states that “more information is needed” in relation to information received from Member States without hotlines “in relation to cases where the web pages hosted abroad are not linked to any criminal proceedings in that Member State.” **In what circumstances and how often do Member States feel that it is appropriate not to launch criminal investigations in relation to crimes against children nor to take rapid and efficient measures, in cooperation with third companies?**

We recommend the Commission call on Member States to take due responsibility in this matter. A single statistic – removals within 72 hours – an impressive 93% for reports processed by EU hotlines and 91% for worldwide hotlines is provided. This leaves many questions unanswered – is it acceptable that removal in nine out of ten cases was possible almost immediately, because there was apparently no ongoing investigation? In relation to the 7% of EU cases where the images were still available after 72 hours, what proportion was still online due to ongoing investigations?

Blocking

Despite the fact that no blocking system is 100% effective, despite that some blocking measures are vastly less or more effective and imply less or more serious surveillance of innocent communications, the Commission fails to acknowledge this nor even to mention the type/s of blocking that are implemented under national procedures.¹ Availability can only be prevented if the image is not online.

The report also fails to report on:

- the number of websites on blocking lists in each country;
- methods, in particular, the use of encryption, for communicating this highly sensitive information to internet providers;
- liability for mistakes in the blocking lists.

Crucially, the report says that “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”. Therefore, any assertion that blocking is effective, necessary, proportionate or even more useful than doing nothing is demonstrably false, as the evidence simply does not exist, according to the Commission.

Blocking safeguards:

According to the Commission, half (7/14) of the countries that have introduced blocking failed to provide meaningful information on safeguards applicable to blocking measures. This is unacceptable.

¹ For more information about different types of blocking, their weaknesses and effectiveness, please see www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

Individual country analyses:

The Commission lists four safeguards: transparency, necessity/proportionality, information to users and possibility of judicial redress. However, the Commission does not analyse the Member States' systems in light of the criteria that the Commission itself identified. This contradicts [what the Commission had promised to do](#): "the Commission will check compliance by the Member States with the requirements of the Directive, in particular with the safeguards that need to be in place".

Greece: the owner of the website may appeal within two months, but there is no indication on whether the owner of the website is informed. No mention is made of why the measure has been assessed to be necessary and proportionate. No mention is made of the proportion of ISPs that undertake blocking, the size of the blocking list, the frequency of updating of the blocking list nor the type of blocking implemented.

Spain: The information provided does not mention blocking. It refers to "closure" websites. No mention is made of why the measure has been assessed to be necessary and proportionate. No mention is made of the proportion of ISPs that undertake blocking, the size of the blocking list, the frequency of updating of the blocking list nor the type of blocking implemented.

Finland: There is no mention of whether (or what proportion of) ISPs actually block on the basis of the police list. Appeals can be made to an administrative court, but no mention is made of whether or how the owner of the website is informed. No mention of the size of the blocking list, the frequency of updating of the blocking list nor the type of blocking implemented.

France: The redress mechanism is not described. No mention is made of whether or how the owner of the website is informed. No mention is made of the proportion of ISPs that undertake blocking, the size of the blocking list, the frequency of updating of the blocking list nor the type of blocking implemented.

Hungary: The notice of blocking is published (in Hungarian, presumably), which is considered adequate to inform any website anywhere in the world that it is blocked in Hungary. No mention is made of the proportion of ISPs that undertake blocking, the size of the blocking list, the frequency of updating of the blocking list nor the type of blocking implemented.

UK: Neither the original assessment by the hotline (which results in an "assessment" and not an order) nor the appeals mechanism is under the authority of a state body. No mention is made of the proportion of ISPs that undertake blocking, the size of the blocking list, the frequency of updating of the blocking list nor the type of blocking implemented.

Back in 2012, EDRi had requested the Commission to bring practices by Member States into line with the Charter. We are in 2017 and are still waiting. We remind Member States and the Commission what Regulation (EU) 2015/2120 establishes:

Recital 13 (second part): “ **The requirement to comply with Union law relates, inter alia, to the compliance with the requirements of the Charter of Fundamental Rights of the European Union (‘the Charter’) in relation to limitations on the exercise of fundamental rights and freedoms. As provided in Directive 2002/21/EC of the European Parliament and of the Council, any measures liable to restrict those fundamental rights or freedoms are only to be imposed if they are appropriate, proportionate and necessary within a democratic society, and if their implementation is subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms, including its provisions on effective judicial protection and due process.**” (emphasis added)

Conclusions and next steps

In its conclusions, the Commission fails to mention the “public authorities, including law enforcement agencies (LEAs) and the judiciary” that it describes as “crucial to implementing the measures in Article 25”. We wholeheartedly agree that public authorities are crucial. We urge the European Parliament to demand that the European Commission prepare a new implementation report that achieves at least minimum standards of diligence.