DRAFT RECOMMENDATIONS FOR PUBLIC PRIVATE COOPERATION TO COUNTER THE DISSEMINATION OF ILLEGAL CONTENT WITHIN THE EUROPEAN UNION

INTRODUCTION

1. Background and purpose of these recommendations

The Council Conclusions of 27 November 2008 on a concerted work strategy and practical measures against cyber-crime invited Member States and the Commission, in particular, to draft, in consultation with private operators, a European agreement model for co-operation between law enforcement agencies and private operators[1].

The recommendations below follow this invitation. They are intended to be endorsed on voluntary basis. They may be complemented, detailed and extended as stakeholders consider appropriate.

In particular, the purpose of this recommendation is to improve the cooperation between Internet service providers[2] that provide services in the European Union, law enforcement authorities, complaint hotlines and other relevant stakeholders in the fight against the dissemination of online illegal content which is made punishable under the Framework Decisions listed below:

- **the Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (OJ L 13 of 20 January 2004, p. 44)[3],**
- **the Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (OJ L 328 of 6 December 2008, p. 55) and**
- **the Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (OJ L 330 of 9 December 2008, p. 21).**

---

[1] OJ L 69, 16.3.2005, p. 67.

[2] For the purpose of these recommendations, we use the definition of service provider included in the Council of Europe Convention of Cybercrime in Article 1 which defines "service provider" in a broad manner as meaning:
i. any public or private entity that provides to users of this service the ability to communicate by means of a computer system, and
ii. any other entity that processes or stores computer data on behalf of such communication service.
This definition was also used in the Council of Europe Guidelines for the cooperation between law enforcement and internet service providers against cybercrime.

[3] On 29 March 2010 the European Commission adopted a proposal for a new Directive on combating sexual abuse, sexual exploitation of children and child pornography. The Directive, if approved, will replace the Framework Decision 2004/68/JHA.

Indeed, these Framework Decisions make punishable respectively, also when it takes place online, the dissemination of child pornography; incitement to racist and xenophobic violence or hatred, and public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism. In particular, the provisions in the section below define these types of behaviour.

2. Relevant provisions defining the illegal content targeted by these recommendations

Article 3 of the Framework Decision on combating the sexual exploitation of children and child pornography reads as follows:

"Offences concerning child pornography

1. Each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of a computer system or not, when committed without right is punishable:

(a) production of child pornography;
(b) distribution, dissemination or transmission of child pornography;
(c) supplying or making available child pornography;
(d) acquisition or possession of child pornography.

2. A Member State may exclude from criminal liability conduct relating to child pornography:

(a) referred to in Article 1(b)(ii) where a real person appearing to be a child was in fact 18 years of age or older at the time of the depiction;
(b) referred to in Article 1(b)(i) and (ii) where, in the case of production and possession, images of children having reached the age of sexual consent are produced and possessed with their consent and solely for their own private use. Even where the existence of consent has been established, it shall not be considered valid, if for example superior age, maturity, position, status, experience or the victim's dependency on the perpetrator has been abused in achieving the consent;
(c) referred to in Article 1(b)(iii), where it is established that the pornographic material is produced and possessed by the producer solely for his or her own private use, as far as no pornographic material as referred to in Article 1(b)(i) and (ii) has been used for the purpose of its production, and provided that the act involves no risk for the dissemination of the material."

Article 1 of the Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law reads as follows:

"Offences concerning racism and xenophobia

1. Each Member State shall take the measures necessary to ensure that the following intentional conduct is punishable:

(a) publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin;
(b) the commission of an act referred to in point (a) by public dissemination or distribution of tracts, pictures or other material;
(c) publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes as defined in Articles 6, 7 and 8 of the Statute of the International Criminal Court, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group;
(d) publicly condoning, denying or grossly trivialising the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group.

2. For the purpose of paragraph 1, Member States may choose to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting.

3. For the purpose of paragraph 1, the reference to religion is intended to cover, at least, conduct which is a pretext for directing acts against a group of persons or a member of such a group defined by reference to race, colour, descent, or national or ethnic origin.

4. Any Member State may, on adoption of this Framework Decision or later, make a statement that it will make punishable the act of denying or grossly trivialising the crimes referred to in paragraph 1(c) and/or (d) only if the crimes referred to in these paragraphs have been established by a final decision of a national court of this Member State and/or an international court, or by a final decision of an international court only.

Article 1 of the Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism reads as follows:

'1. Article 3 shall be replaced by the following:

"Article 3

Offences linked to terrorist activities

1. For the purposes of this Framework Decision:

(a) "public provocation to commit a terrorist offence" shall mean the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;
(b) "recruitment for terrorism" shall mean soliciting another person to commit one of the offences listed in Article 1(1)(a) to (h), or in Article 2(2);
(c) "training for terrorism" shall mean providing instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the offences listed in Article 1(1)(a) to (h), knowing that the skills provided are intended to be used for this purpose.

2. Each Member State shall take the necessary measures to ensure that offences linked to terrorist activities include the following intentional acts:

(a) public provocation to commit a terrorist offence;
(b) recruitment for terrorism;
(c) training for terrorism;
(d) aggravated theft with a view to committing one of the offences listed in Article 1(1);
(e) extortion with a view to the perpetration of one of the offences listed in Article 1(1);
(f) drawing up false administrative documents with a view to committing one of the offences listed in Article 1(1)(a) to (h) and Article 2(2)(b).

3. For an act as set out in paragraph 2 to be punishable, it shall not be necessary that a terrorist offence be actually committed."

[...]'

3. Scope of these recommendations

The recommendations are intended to clarify notice and take down procedures. They do not refer to filtering or blocking methods.

Therefore, the reference to the dissemination of illegal content in the recommendations must be understood as strictly limited by the definitions of criminal offences provided in the provisions above. In this sense, the recommendations do not cover:

- **the dissemination of other types of illegal or unlawful content which are not included in the Framework Decisions listed above, nor**
- **the dissemination of content which may be considered harmful or undesirable.**

Moreover, these recommendations do not include any restriction to online communications which is not defined as a criminal offence under the Framework Decisions listed above nor do they censor online communications in any other way.

4. Relevant provisions in the Directive on electronic commerce

In the context of notice and take down procedures, it is necessary to bear in mind the exemptions of liability for Internet service providers set out in Articles 12 to 15, of the **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'), OJ L 178, 17.7.2000, p. 1.** These provisions belong to Section 4 of the Directive: "Liability of intermediary service providers" and read as follows:

'Article 12

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13

"Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;
(b) the provider complies with conditions on access to the information;
(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14

Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15

No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'

Recitals 42 to 49 in the preamble to the Directive on electronic commerce should also be taken into consideration:

(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.

(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.

(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a

specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

(49) Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes.

5. The content of these recommendations

In order to clarify notice and take down procedures, the recommendations below define the roles of the different stakeholders that may be involved in notice and take down procedures and specify whom to contact and how to proceed in the different possible scenarios.

With the purpose of further facilitating contacts between stakeholders, the creation of a list of contact persons designated by the members endorsing the recommendations is foreseen. The Commissions offers to provide a restricted portal where this list should be made available.

Furthermore, the recommendations refer to the introduction of liability exemptions for Internet service providers in the terms of service which are part of the contracts with their clients. Such exemptions would ensure that Internet service providers are not held liable in case of termination or suspension of a contract following notice and take down procedures.

Finally, the recommendations encourage law enforcement authorities, Internet service providers and complaint hotlines to organise or participate in training programmes to counter online illegal content more efficiently as well as to promote awareness campaigns addressed to Internet users, which should be encouraged to report the illegal content they come across.

RECOMMENDATIONS

1. DEFINITION OF ROLES

1. Fighting online criminal activities, including the transmission, over the Internet, of illegal content, is the task of law enforcement authorities.

2. Internet service providers must remove or disable access to illegal content with due diligence when requested by law enforcement authorities or as otherwise required by law.

3. However, actively seeking facts or circumstances indicating the use of their services for criminal purposes is not the task of Internet service providers.

4. Internet service providers are encouraged to develop a close partnership with complaint hotlines. The use of complaint hotlines' expertise would benefit Internet service providers in ensuring their systems are as clean as possible.

5. Complaint hotlines are reporting points for illegal content that receive complaints from members of the public coming across illegal content and cooperate with law enforcement authorities to fight illegal content in an agreed manner or as otherwise required by law, which may involve the notification of illegal content to the internet service provider.

6. Citizens should be encouraged to notify illegal content or content that raises reasonable doubts about its legality whenever they come across it. For this purpose, internet service providers, hotlines and law enforcement authorities should facilitate online notifications.

2. NOTICE AND TAKE DOWN

2.1 WHOM TO ADDRESS

1. Public authorities, Internet service providers, hotlines and other members endorsing these recommendations should designate a contact person/contact persons.

2. The list of contact persons will be made available through a restricted portal, fully compliant with data protection rules applicable in the EU.

3. Every member is responsible for the accuracy of the data provided and must communicate eventual changes with due diligence.

4. The contact persons designated should be available, at a minimum, during working days.

2.2 DIFFERENT SCENARIOS: HOW TO PROCEED

2.2.A) Request of law enforcement authorities to interrupt the transmission of the content uploaded by the client or to disable access to it by means of a legal injunction or a formal legal order

The request of law enforcement authorities, by means of a legal injunction or a formal legal order, to interrupt the transmission of the content uploaded by the client or to disable access to it is imperative. There is an obligation of Internet service providers to comply with it.

Unless another time limit is specified in the legal injunction/formal legal order or is otherwise required by law, a reasonable time limit by which the Internet service providers should either take down the notified content or, in case they consider the content legal, inform the body that has notify them together with the reasons for this is two working days.

2.2.B) Notification of content uploaded by the client as illegal or allegedly illegal

2.2.B.1) Notification by law enforcement authorities, a complaint hotline or other body duly authorised or tasked under national law to monitor Internet content

Internet service providers should take the content down unless they consider that the notified content is legal and duly inform the body that has notified them, together with the reasons for this.

A reasonable time limit by which the Internet service providers should either take down the notified content or, in case they consider the content legal, inform the body that has notified them together with the reasons for this is two working days.

2.2.B.2) Notification by citizens

Internet service providers should take down the notified content if the notification leaves no doubts about the illegality of the content. Internet service providers should subsequently inform hotlines or law enforcement authorities about this action.

If the Internet service provider considers that the content notified may be legal, it should forward the notification to law enforcement authorities, hotlines or bodies duly authorised or tasked under national law to monitor Internet content. These should evaluate the notification and issue, when appropriate, a request or a notification as indicated above (A and B1).

A reasonable time limit by which the Internet service providers should take down the notified content or, if they consider that the content notified may be legal, forward the notification to law enforcement authorities, hotlines or bodies duly authorised or tasked under national law to monitor Internet content is two working days.

3. LIABILITY EXEMPTIONS IN THE TERMS OF SERVICE

Internet service providers can, in accordance with Article 12-15 of the Directive on electronic commerce, include in their terms of service appropriate liability exemptions in case of suspension or termination of the contract following:

a) The request of law enforcement authorities to interrupt the transmission of the content uploaded by the client or to disable access to it by means of a legal injunction or a formal legal order.

b) The notification by law enforcement authorities, a complaint hotline or any other body duly authorised or tasked under national law to monitor Internet content, of content uploaded by the client which is illegal or allegedly illegal. .

4. TRAINING AND RAISING AWARENESS

1. Law enforcement authorities, Internet service providers, complaint hotlines and other bodies duly authorised or tasked under national law to monitor Internet content should be encouraged to organise and participate in training programmes on fighting online illegal content, in particular through efficient notice and take down procedures.

2. Law enforcement authorities, Internet service providers, complaint hotlines and other bodies duly authorised or tasked under national law to monitor Internet content should be encouraged to organise and participate in information campaigns addressed to citizens, to make them aware of the dissemination of illegal content through the Internet and the importance of the role they can play by notifying illegal content or content that raises reasonable doubts about its legality whenever they come across it