27/10/2020

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online

Questions for written answer to the Commission by the EP rapporteur Birgit Sippel, S&D, following up on a first set of questions sent on 28 September 2020 and to which answers were received on 9 October 2020

Please note: In order to not cause any unnecessary delay, we kindly ask for written answers to each individual question, no general replies, or grouping of several questions, please. Deadline for replies: **6 November 2020**. The list below is not intended to be exhaustive and should not prevent the rapporteur or her shadows from raising additional questions and issues at a later stage.

A. Follow-up questions to written replies sent on 9 October

► *2. Since there is no impact assessment, can the Commission provide a complete mapping of the different national rules and practices currently in place regarding the detection of CSAM?*

Response of the Commission's services:

The Commission's services are currently finalising a mapping of such rules in Member States and it will be transmitted to the European Parliament as soon as it is completed. (...)

Follow-up questions:

1) ***► How is it possible for the Commission to reach the conclusion in a draft legislative Union act that "Lack of Union action on this issue would risk creating fragmentation should Member States adopt diverging national legislation" (p. 3 of the proposed regulation) if the Commission cannot provide a list of what the current different rules and practices are?***

Once the European Electronic Communications Code enters into force, the ePrivacy Directive will apply to number-independent interpersonal communications services for

the first time. Member States wishing to allow the continuation of voluntary measures for the detection and deletion of CSA online could do so by establishing a restriction to the rights and obligations, as provided for in Article 15(1) of the ePrivacy Directive, which permits Member States to restrict the scope of certain rights and obligations provided for in the Directive through national legislation provided certain conditions are met. It is unlikely that such measures would be adopted by all Member States by 21 December 2020, and it is similarly unlikely that the scope and safeguards of these measures would be aligned to the extent that fragmentation would be avoided. In addition, in contrast to traditional telecommunications providers which usually have a presence and distinct legal entity in each Member State market given the national licensing processes for telecommunications providers, number-independent interpersonal communications services are often provided internationally, without specifications for national markets. Union legislation is therefore the only way in which a derogation from the application of provisions of the ePrivacy Directive for certain processing activities can be achieved to avoid fragmentation which would negatively affect the internal market.

2) ► When exactly will the Commission be able to transmit a mapping of such rules to the Parliament?

Please see annex.

***

► *11. How does the Commission justify this departure from the criminal law provisions of the child sexual abuse directive?*

Response of the Commission's services:

At the outset, it must be emphasised that the proposed Regulation is not a criminal law instrument.
(...)

Follow-up questions:

3) ► If this is not a criminal law definition and therefore not necessarily illegal in all Member states, what exactly happens in case of a positive hit? More precisely: What would a Member state do with a hit indicating solicitation of a child according to the proposed definition but which is not followed up by a material act and as such potentially not punishable in the Member state concerned? Can the Commission provide an overview of what the legal situation in this regard in Member states is?

The situation in Member States where such act is not necessary illegal would be similar to any situation in which a report is made to law enforcement authorities of a conduct which, upon investigation, does not constitute a criminal offence. In such a situation, it is to be expected that the investigation would be discontinued and no criminal proceedings would be initiated.

However, it is to be noted that a number of Member States have gone beyond the minimum requirements of the Directive and have criminalised certain types of attempts of grooming (e.g. Germany).[1] In that case, it would not therefore be required to complete the material act cited.
In addition, the identification of a situation where a child was at risk – even if that risk did not materialise in child sexual abuse in the specific instance and is therefore not punishable in that Member State – would allow the company to take steps to protect the child, e.g. by preventing a continuation of the communication or by informing the child of the potential risk.

4) ► How can an act which is not a crime (in this case "solicitation of a child" as per the proposed regulation, which is neither codified in Union criminal law nor necessarily in national criminal law), be a justification for the interference with the fundamental rights to privacy and data protection, also taking into account the ECJ case law on this matter?

As previously noted, the definition of solicitation laid down in Article 6 of the Directive is not suited for service providers to use in practice. If Article 6 of the Directive were to apply, service providers would have to establish the existence of material acts leading to a meeting offline.

While solicitation of children under the proposed Regulation does not, in itself, constitute a criminal offence, the purpose of its inclusion is to enable in particular the prevention, but also the investigation, detection and prosecution of criminal offences which may evolve from such conduct. Relevant Union legislation such as the General Data Protection Regulation, the ePrivacy Directive and the Law Enforcement Directive explicitly acknowledge that the processing of personal data for the prevention, investigation, detection or prosecution of criminal offences can be legitimate in the context of the rights to privacy and data protection.

In particular, given the fact that it may take just a few hours from the start of the grooming activity to the child being sexually abused (online and/or offline), a company report enabling the timely detection of grooming, can prevent the abuses from taking place. Given the significant risk arising from grooming and the long-term negative consequences on the child once the crime is complete, effective prevention is essential. The high risk has also been recognised by Member States that have gone beyond the minimum requirements of Directive 2011/93 and criminalised certain types of attempts of grooming beyond the requirements of Article 6(2) of Directive 2011/93.

***

► 20. Will the scanning for solicitation of children require retrospective searches and therefore the retention of communication by providers as, in contrast to hashing technology, solicitation of a child is something you would only be able to establish over time?

[1] Germany has criminalised one specific type of attempt, namely if the completion of the criminal offence fails because the addressee is actually not a child.

Response of the Commission's services:

No. According to Microsoft, the technology is based on "historic" chats, as opposed to "real-time" chats, with "historic" dating typically no more than a day. With that information, the tool offers risk scores for the conversation, which would trigger an alert over a certain threshold.

Follow-up question:

5) ► This response seems a bit contradictory. How is searching in "historic" chats not a retrospective search?

The tool uses "historic" chats as opposed to "real-time" chats with "historic" dating typically no more than a day and as such the tool does not necessitate retention of communication by providers for an extended period.

As pointed out in question 4), the grooming of a child can take place in just a few hours.

***

► *40. Does the scope of the proposal cover detecting illegal content in private clouds, for example by photo DNA ?*

Response of the Commission's services:

The scope of the present proposal is strictly limited to number-independent interpersonal communications services. Private clouds are in principle storage and therefore normally not number-independent interpersonal communications services. The qualification of the service depends of course on the facts of the individual case.

Follow-up question:

6) ► Microsoft states that it uses PhotoDNA on its cloud storage.2 Can the Microsoft Cloud be considered a number-independent interpersonal communication service and thus be covered by the proposed derogation?

It is ultimately the Court of Justice that will interpret the European Electronic Communications Code (EECC), therefore the replies by the Commission's services

[2] "4. (...) Microsoft uses PhotoDNA on several of its services, including its OneDrive cloud storage service, the Xbox Live gaming platform, Bing search, and the LinkedIn professional social network. PhotoDNA is leveraged to scan certain user-generated content against a database of "hashes" (unique digital fingerprints) of known images of child sexual abuse to identify duplicate images.", affidavit by Courtney Gregoire, Chief Digital Safety Officer at Microsoft Corporation.

given below regarding the EECC should not be perceived as its interpretation and do not bind the Commission.

The conditions to constitute a 'number-independent electronic communications service' are provided in Art. 2(5) and 2(7) of the EECC. Accordingly, if the services are provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and do not connect with publicly assigned numbering resources (a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans), they would constitute a number-independent interpersonal electronic communications service. "cloud storage services" are normally not intended for direct interpersonal and interactive exchange of information, but for storage of information. Moreover, in line with Recital 17 EECC, even if "cloud storage services" might technically be used for direct interpersonal and interactive exchange of information between a finite number of persons, from an objective end-user's perspective such technical facility would most likely be a minor and purely ancillary feature to the "storage" service. As a result, it could be argued that cloud storage services would normally not be considered a number-independent interpersonal communication service. As noted earlier, the legal qualification of a given service depends however on the facts of each individual case.

***

► *51. Apart from E-Mail and Messaging services, which types of services constitute "number-independent electronic communications services"? For example, are online games, services such as Skype, the provision of Internet access, by fixed line or by wifi, dating apps, apps used to find and communicate with people in the neighborhood, based on the user's location, "number-independent electronic communications services" and covered by the scope of the proposed regulation?*

Response of the Commission's services:

Art. 2(5) of the European Electronic Communications Code (EECC),[3] states that 'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service'. Art. 2(7) states that 'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans'.

[3] Directive (EU) 2018/1972, Articles 2(5) and (7).

Whether a service constitutes a number-independent interpersonal electronic communications service will depend on the specifics of that service, and so it is only possible to respond to the examples above in general terms. Recitals 15-18 of the EECC provide guidance in that respect.
In particular:

Recital 17 of the EECC clarifies that, in exceptional circumstances, a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms 'minor' and 'purely ancillary' should be interpreted narrowly and from an objective end-user's perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service. These elements have to be assessed on a case-by-case basis.

(...)

Follow-up questions:

7) ► Microsoft states that it uses PhotoDNA on LinkedIn.[4] Can LinkedIn be considered a number-independent interpersonal communication service and thus be covered by the proposed derogation?

It is ultimately the Court of Justice that will interpret the EECC, therefore the replies by the Commission's services given below regarding the interpretation of the EECC should not be perceived as its interpretation and do not bind the Commission. Recital 17 of the European Electronic Communications Code (EECC) indicates that services such as linear broadcasting, video on demand, websites, social networks, blogs, or exchange of information between machines, should not be considered to be interpersonal communications services. However, as noted earlier, the legal qualification of a given service depends on the facts of each individual case.

[4] "4. (...) Microsoft uses PhotoDNA on several of its services, including its OneDrive cloud storage service, the Xbox Live gaming platform, Bing search, and the LinkedIn professional social network. PhotoDNA is leveraged to scan certain user-generated content against a database of "hashes" (unique digital fingerprints) of known images of child sexual abuse to identify duplicate images.", affidavit by Courtney Gregoire, Chief Digital Safety Officer at Microsoft Corporation.

8) ► Can the LinkedIn chat function be considered a minor and purely ancillary feature to another service (the LinkedIn network) that for objective technical reasons cannot be used without that principal service?

According to Recital 17 of the EECC, in exceptional circumstances a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms 'minor' and 'purely ancillary' should be interpreted narrowly and from an objective end-user's perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users.

In light of Recital 17 of the EECC, the LinkedIn chat function can be considered as a minor and purely ancillary feature to the main service of LinkedIn if, for objective technical reasons, it cannot be used without that principal service, its integration is not a means to circumvent the applicability of the rules governing electronic communications services, its objective utility for an end-user is very limited, and, in reality, it is rarely used by the end-users. As noted earlier, the legal qualification of a given service depends however on the facts of each individual case.

9) ► Are videoconferencing services, including those used for medical consultations, "number-independent electronic communications services" within the scope of the proposed derogation?

It is ultimately the Court of Justice that will interpret the EECC, therefore the replies by the Commission's services given below regarding the interpretation of the EECC should not be perceived as its interpretation and do not bind the Commission. The conditions for constituting a 'number-independent electronic communications service' are provided in Art. 2(5) and 2(7) of the European Electronic Communications Code (EECC). Therefore, under the condition that such videoconferencing services are provided for remuneration, as explained in Recital 16 of the EECC, and enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, it can be argued that they constitute a (number-independent) interpersonal electronic communications service. Such services will therefore constitute number-independent interpersonal communications service if they are interpersonal communications services, which do not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which do not enable communication with a number or numbers in national or international numbering plans, as provided in Art. 2(5) of the EECC. Recitals 15-18 of the EECC provide guidance in that respect. As noted earlier, the legal qualification of a given service depends however on the facts of each individual case.

10) ► On the answers send in early October the Commission named only U.S.-based companies by example to the questions which number-independent electronic communication services filter communications content for potential grooming/solicitation and/or previously classified and/or yet unknown CSEM. Has the Commission any knowledge about companies and service providers based in Europe who are using these voluntary measures for the detection and reporting of child sexual abuse online and the removal of child sexual abuse material?

The service providers listed in the Commission's previous response also operate in the EU, where they provide the vast majority of reports of child sexual abuse in the EU, given their position in terms of market share of number-independent interpersonal communication services. They report to law enforcement authorities in the EU through the US national centre NCMEC, as there is no such centre in the EU yet. Whereas US law requires US-based providers to report infringing content to NCMEC, there is no comparable obligation on EU-based providers to report infringing content to a centralised reporting point.

Last year, these services sent to NCMEC more than 725 000 reports concerning the EU (e.g. images exchanged in the EU, victims in the EU, etc.), up from 23 000 reports in 2010. Those reports sent last year included more than 3 million images and videos.

11) ►On which legal basis and under which conditions do companies share (transfer) the information with the US (NCMEC)?

When companies aim at transferring personal data to third countries, they need both a legal basis for processing under Article 6 GDPR and a legal ground for transfer in line with the provisions of Chapter V of the GDPR. According to Article 44 GDPR, companies must ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined when personal data is shared with other public or private entities in another third country.

While companies have a direct responsibility to determine whether there is an appropriate legal basis and one of the grounds/instruments for data transfers is available, it is for the data protection authorities to assess whether these transfers are lawful and to enforce any possible infringements of the GDPR.

This proposal does not create a new legal ground for processing or modify the existing legal basis in relation to international data transfers.

***

► *57. Which number-independent electronic communication services filter communications content for potential grooming/solicitation, to the knowledge of the Commission? (please provide names of services!)*

Response of the Commission's services:

According to the information available to the Commission's services, number-independent electronic communications services which currently voluntarily detect grooming/solicitation in their services include Microsoft's Xbox. Recital 17 of the EECC clarifies that, in exceptional circumstances, a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms 'minor' and 'purely ancillary' should be interpreted narrowly and from an objective end-user's perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service. These elements have to be assessed on a case-by-case basis.

(...)

Follow-up questions:

12)► Does this response mean that the Commission does not consider that Microsoft's Xbox would fall within the scope of the proposed derogation?

It is ultimately the Court of Justice that will interpret the EECC, therefore the replies by the Commission's services given below regarding the interpretation of the EECC should not be perceived as its interpretation and do not bind the Commission. According to the information available to the Commission's services, the services, which currently voluntarily detect grooming/solicitation in their services include Microsoft's Xbox. Recital 17 of the EECC clarifies that, in exceptional circumstances, a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As a general rule, exceptions are to be interpreted restrictively. An interpersonal communications feature could, for instance, be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service. These elements have to be assessed on a case-by-case basis. In light of Recital 17 of the EECC, an online game service itself does not appear to interpersonal communications service. Recital 17 further indicates that the communications channel in an online game service might be considered as a minor and purely ancillary feature

and, therefore, not constitute an interpersonal communications service. However, the concrete assessment has to be made case-by-case by the competent national regulatory authorities, and ultimately the courts.

13) ► Why would the proposed derogation include "solicitation of a child" when grooming technology currently seems to be almost exclusively used in game chats, which usually would be an ancillary feature and thus not fall within the enlarged scope of the ePrivacy directive and thus neither in that of the derogation?

Whether the Xbox chat function, which works on consoles, mobile devices and PCs independently of individual games offered on the Xbox, or other games chat functions with different features fall outside the enlarged scope of the ePrivacy directive has to be assessed case-by-case by the competent national regulatory authorities, and ultimately the courts, and cannot be determined in abstracto. Recital 17 of the EECC clarifies that, in exceptional circumstances, a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As a general rule, exceptions are to be interpreted restrictively. An interpersonal communications feature could, for instance, be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users.

In addition, the proposal's sole aim is to enable providers of number-independent interpersonal communications services to continue using specific technologies and continue their current activities to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services, pending the adoption of the announced long-term legislation.

Providers use grooming detection technology in a variety of number-independent electronic communication services. As included in the annex with NCMEC data, the breakdown of the grooming reports received in the EU in 2019 is the following:

Type of Platform	Number of Reports
Chat or Messaging	55
Social Media - Messaging Possible	175
Online Gaming - Messaging Possible	5
Other	5
Grand Total	**240**

Whereas Microsoft seems to be using its anti-grooming technology in its Xbox service, other providers such as Facebook have developed their own anti-grooming technology.

In addition, Thorn makes available Microsoft's technology to other companies (Anti-grooming starter kit), which may use it in services other than online game chats. The proposed exemption would create the required legal certainty for providers to continue their efforts to protect children provided they meet the relevant conditions.

14)► Of the 240 grooming reports in the EU in 2019, how many were detected by the automated tool developed by Microsoft?

The Commission services do not have that information. According to NCMEC, the breakdown of grooming reports in the EU by type of platform was the following:

Type of Platform	Number of Reports
Chat or Messaging	55
Social Media - Messaging Possible	175
Online Gaming - Messaging Possible	5
Other	5
Grand Total	**240**

In addition to Microsoft, other service providers such as Facebook have developed their own anti-grooming tools.

***

► *67. Can the Commission share the assessment of its legal service with regards to the proportionality and necessity of the proposed legislation on scanning all communication content of all users, in particular in light of the CJEU case-law on data retention and Schrems?*

Response of the Commission's services:

This proposal, as any legislative proposal adopted by the Commission, has been assessed by the Commission's legal service. That assessment covered all relevant legal aspects, including compliance with the Union legal principle of proportionality.

This proposal does not create a new legal ground for processing or modify the existing legal basis in relation to data retention or international data transfers.

Follow-up question:

15)► Will the Commission share the assessment of its legal service with regard to the proportionality and necessity and respect for fundamental rights of the proposed legislation on scanning all communication content of all users?

The Commission's Legal Service has assessed this proposal, also in view of its compliance with the principle of proportionality. The Commission's Legal Service assessments are internal documents for the sole purpose of assisting the Commission and its services, and are not made public or shared with other institutions, which have their own Legal Services.

B. Additional questions

In its judgment in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others of 6 October 2020, the CJEU decided that in order to meet the requirement of proportionality, national rules i.e. on automated analysis of communications need to be limited to situations in which a Member State is facing a serious threat to national security, or to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities.

16) ► Would the Commission agree that these requirements apply to the proportionality of automatically analyzing the content of communications as well? Would the Commission agree that not only legally mandated but any analysis of private communications (including "voluntary" filtering) would need to be proportionate in line with the judgment in order to be GDPR-compliant?

The judgment referred to concerns, *inter alia,* the requirement for providers of electronic communications services to carry out, at the request of competent authorities, the automated analysis and real-time collection of traffic and location data in the specific context of threats against national security, subject to a number of conditions and safeguards that must be laid down in law and observed (limited time of operation, independent judicial control, specific predefined selection criteria, periodic re-examination of the selection criteria to ensure that they are reliable and up-to-date, human verification of results of automated processing). Thus, whilst the Commission services would certainly agree that the principle of proportionality and the GDPR need to be respected, the judgment relates to a different situation than the one at issue here, in particular in view of the fact that the proposed Regulation does not impose any obligations on the service providers concerned.

In addition, the proposed Regulation includes requirements and safeguards, such as the respect of the limitation of the processing to what is strictly necessary, and for human review of the results of automated processing. Moreover, as stated in Recital 10 of the proposal, the GDPR applies to the processing of personal data in connection with the provision of electronic communications services by number-independent interpersonal communications services, including the requirement to carry out an assessment of the impact of the envisaged processing operations, where appropriate pursuant to Article 35 of GDPR prior to the deployment of the technologies concerned. In this regard, any processing of personal data within the context of the proposal, including the analysis of private communications, needs to comply with all GDPR principles.

17) ► Will the providers of number-independent electronic communications services be obliged to respect the confidentiality of electronic communications content as of 21/12/2021 due to the Electronic

Communications Code, or will there be no direct horizontal effect on those providers, as long as Member States have not transposed the EECC into national legislation?

The ePrivacy Directive applies to the processing of personal data in connection with the provision of publicly available electronic communication services. The definition of electronic communication service is currently to be found in Article 2, point (c), of Directive 2002/21/EC of the European Parliament and of the Council (Framework Directive). By virtue of Article 125 of Directive (EU) 2018/1972 of the European Parliament and of the Council (EECC), Directive 2002/21/EC, among others, is repealed, with effect from 21 December 2020, **without prejudice to the obligations of the Member States relating to the time-limits for the transposition into national law and the dates of application of the Directives,** set out in Annex XII, Part B of the EECC.

18) ► Can the Commission confirm that the Irish national law currently does not extend the ePrivacy rules to OTT communications service providers?

According to the information available to the Commission services, the ePrivacy Directive is transposed in Ireland via law "S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011". This Regulation refers to S.I. No. 333/2011 - European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011, which transposes Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). The 'electronic communications service' is defined as follows:
'*electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes—*
(a) services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, and
(b) information society services, as defined in Article 1 of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 , which do not consist wholly or mainly in the conveyance of signals on electronic communications networks';

It would seem that the Irish national law does not currently extend the ePrivacy rules to OTT communications service providers.

19) ► Is there draft legislation in Ireland to transpose the Electronic Communications Code? If so, is it to allow for indiscriminate filtering of private communications contents by OTT services?

According to information provided by the Irish authorities to the Commission services, Ireland is working towards transposing the European Electronic Communications

Code. Secondary legislation transposing the EECC has been drafted and Ireland expects this legislation to be adopted before the deadline for transposition.

20) ► Does the Commission take the view that according to Article 3 of the eCommerce directive, the only provisions on communications secrecy applicable to companies established in Ireland are Ireland's?

The Commission does not take this view, for the reason that Article 1(5)(b) of the eCommerce Directive excludes its application to "questions relating to information society services covered by Directives 95/46/EC and 97/66/EC [since repealed and replaced by the General Data Protection Regulation and the ePrivacy Directive, respectively]".

The Commission names the following number-independent electronic communications services, which currently voluntarily detect known child sexual abuse material or child grooming in their services: Facebook Messenger, Gmail, Yahoo Messenger, Kik Messenger and Microsoft Xbox.

21) ► Do the providers of these services have a legal representation in the EU and which Member States are they located in?

The providers of the majority of the above services are established in the EU, and are therefore not required to designate a representative in writing under Article 27 of the General Data Protection Regulation.

22) ► If not: How does the ePrivacy Directive apply to them in the first place, since there is no market location principle in it?

Article 1(2) of the ePrivacy Directive provides that this Directive particularises and complements Directive 95/46/EC that was replaced by the GDPR. Article 27 of the GDPR sets an obligation to designate in writing a representative in the Union. In accordance with Article 3, the ePrivacy Directive applies to the provision of publicly available electronic communications services within the EU, irrespective of the location of the provider's headquarter.

23) ► Have any of these providers announced that in the absence of a derogation, they would stop filtering on 21 December 2020?

The Commission services are not aware of providers of number-independent interpersonal communications services that have made such announcement That said, providers of number-independent interpersonal communications services have stressed the importance of the proposed derogation in allowing voluntary measures to continue.

24)► Which CSEM detection technologies do each of these operators use?

Technologies used for the detection of child sexual abuse online by these operators include PDQ and TMK+PDQF (Facebook)[5], PhotoDNA (Kik[6]. and others)[7] and grooming detection technology[8] (Microsoft), Content Safety API[9] and AI technology[10] (Google).

25)► According to Microsoft, the purely automated detection through their grooming tool is 88% accurate. Is this the rate of false negatives (12% of grooming conversations are not detected) or of false positives (12% of detected conversations do not constitute child grooming)? Please disclose both the true and false negatives rates.

According to Microsoft, this is the rate of false positives.

The rate of false negatives cannot be established as there are no parallel checks of the content that would identify the conversations containing grooming that were not flagged as such by the anti-grooming tool. Also, the anti-grooming tool does not detect what every conversation is about and therefore is unable to wrongly flag a grooming conversation as a conversation about something else. As explained in the technical annex, these technologies to detect child sexual abuse online answer the question "is this content likely to be child sexual abuse, yes or not?" not the question "what is this conversation about?" In other words, the tools look for specific indicators of possible child sexual abuse and are only able to determine whether a conversation is likely to be grooming.

► *According to Thorn, its Safer tool has an accuracy of 99% in the detection of known and unknown material in its automated part.*

26)- Is this the rate of false negatives (1% of CSAM are not detected) or of false positives (1% of detected conversations do not contain CSAM)? Can you disclose both the true and false negatives rates, please?

According to Thorn, this is the rate of false positives, i.e. 1% of the content flagged as CSAM will end up being non-CSAM.

The rate of false negatives cannot be established (i.e. actual CSAM that is not flagged as such or that is flagged as something else), since there are no parallel checks of the content that would identify the CSAM not flagged by the Safer tool. Also, this technology does not identify what every image is (e.g. a dog, a house, a car) and therefore is unable to wrongly flag a CSAM image as an image about something else. As explained in the technical annex, these technologies to detect

[5] Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer
[6] Using Microsoft's PhotoDNA to protect Kik users
[7] PhotoDNA
[8] Microsoft shares new technique to address online grooming of children for sexual purposes
[9] Fighting child sexual abuse online
[10] Using AI to help organizations detect and report child sexual abuse material online

child sexual abuse online answer the question “is this content likely to be child sexual abuse, yes or not?” not the question “what is this picture about?” In other words, the tools look for specific indicators of possible child sexual abuse and are only able to determine whether it is a CSAM image or video.

27)- What is the rate of false positives and negatives regarding the unknown material detection only?

According to Thorn, the rate of false positives of the detection of unknown material through classifiers is 1%.

28)- How many false positives have been reported via Thorn’s “Safer API”?

The Commission’s services do not have this information.

29)- What happens concretely in the case of a false positive or in case an individual receives CSAM without wishing so?

In the case of a false positive, there are up to four verifications that can detect it and simply stop the process:

1. At the company, through human review, before the material is reported to NCMEC.
2. At NCMEC, through human review, before the report is forwarded to law enforcement, depending on the type of report.
3. At Europol, through human review, before the report is forwarded to national law enforcement, depending on the type of report and the destination country (some countries receive the reports directly from NCMEC).
4. At the recipient Member State, through human review, by the law enforcement agency in charge of the case.

If an individual receives child sexual abuse material without wishing so, it is unlikely that a criminal investigation will be started, if the intent, which is key to determine criminal responsibilities, is not present. Company policies in this type of situations may vary, and they typically have in place redress mechanisms so that users who think that they have been wrongly accused, can refer their case to the companies for review. In any case, the onus should not be on the user to prove he or she is innocent, but on the service provider to ensure the technology used is reliable. It is also noted that in practice, most if not all providers will notify the user once an image is removed.

30)► Is the Commission aware of employees or contractors of communications service providers that have illegally disclosed customer data or

communications in the past? Could the review of private communications thus contribute to the spread of child sexual exploitation material?

In the context of voluntary measures by providers of number-independent interpersonal communications services for the detection of child sexual abuse material online, the Commission services are not aware of cases where employees or contractors of these services have illegally disclosed customer data or communications in the past.

31) ► Why does the title of the proposed legislation – as opposed to Directive 2011/92/EU – mention "child sexual abuse" only and lacks the second element of "sexual exploitation of children"?

The title of the proposal refers to "child sexual abuse online", as defined in Article 2(2) of the proposal. This definition encompasses behaviours that relate to both child sexual abuse (i.e. child pornography or child sexual abuse material) and child sexual exploitation (i.e. pornographic performances) as defined in Directive 2011/93/EU.

The proposal refers to child sexual exploitation in the explanatory memorandum and several recitals, notably on recital 4, where it also refers to the EU strategy for a more effective fight against child sexual abuse. Similarly to the proposal, although this strategy refers only to child sexual abuse in its title, it also covers the sexual exploitation of children, as clarified in footnote 9 of the strategy.

32) ► Do Facebook Messenger, Yahoo Messenger, and Kik Messenger filter communications content for yet unknown CSEM (child sexual exploitation material)?

According to NCMEC the above providers have reported unknown child sexual exploitation material that do originate in communications.

33) ► Is the Commission aware of any number-independent electronic communications services that implements Thorn's "safer" tool to filter communications content for yet unknown CSEM (child sexual exploitation material)?

According to Thorn, its Safer tool works as part of the 3 step process described below:

1. Detection through hashing technology. Safer uses PhotoDNA (perceptual hash), MD5 (exact match), and the Safer Hash (newer perceptual hash, not a classifier).
2. Human review, to confirm whether the detected, possible CSAM is actually CSAM. To assist the human review process, Safer uses classifiers to determine the level of abuse and prioritize the images that come in through initial detection. This helps the manual reviewers queue the reports appropriately.

3. Reporting to NCMEC, which again analyses the reports to double check that the they do contain CSAM.

Therefore, the first detection of CSAM is done through hashing, and new material is only detected in the messages already flagged for review.

As described in the technical annex already transmitted, other tools making use of classifier and AI technology to detect previously unknown CSAM include Google's Content Safety API[11], and Facebook's AI technology[12].

34) ► How many persons use Facebook Messenger, Gmail, Yahoo Messenger, Kik Messenger and Microsoft Xbox? And how many users of these services per year are reported to NCMEC?

The Commission services do not have this information.

Whereas in 2019 NCMEC received nearly 17 million reports, each report may include information of one or several users, and some reports may refer to the same user(s).

35) ► Can the Commission confirm that the proposed legislation would derogate from the ePrivacy directive, but not from national law transposing it?

The proposed Regulation provides for a temporary derogation from Article 5(1) and Article 6 of the ePrivacy Directive. It restricts the right to protection of the confidentiality of communications and derogates from the decision taken with the adoption of the European Electronic Communications Code (EECC) to subject number-independent interpersonal communications services to the same rules as all other electronic communications services as regards privacy. These services are not covered by the scope of the ePrivacy Directive until 21 December 2020 and will fall into the scope of the ePrivacy Directive by virtue of the definitions of the EECC as from that day.

The ePrivacy Directive currently refers to the definition of 'electronic communications service' in the Framework Directive that does not encompass number-independent interpersonal communications services.

Accordingly, the proposed Regulation would derogate from the ePrivacy Directive, but not from the national laws transposing the Directive as those laws stand before the transposition of the new definition of the EEEC. The proposed Regulation makes it clear that those laws should not be amended so as to cover also the services at issue here. In any event, by virtue of being a directly applicable measure of Union law, it would take precedence over any national laws that are not compatible with it.

[11] Fighting child sexual abuse online

[12] See here and here for more information on Facebook's tool to proactively detect child nudity and previously unknown child exploitative content using artificial intelligence and machine learning.

36) ►Did the Commission involve any EU based NGOs or companies before proposing this legislation? (please list)

The Commission's consultations with companies in relation to this proposal have focused on the major service providers which contribute over 95% of the reports made to NCMEC, and which also operate in the EU. Facebook, Microsoft and Google contributed 16,457,663 reports to NCMEC in 2019, representing 97.7% of the 16,836,694 reports received from all service providers (including providers of number-independent interpersonal communications services as well as other service providers, see annex on 2019 Reports by ESP with NCMEC data previously provided).

The Commission took note of the views of various NGOs, both on the child protection and the privacy areas.

ANNEX: mapping of national rules and practices currently in place regarding detection of CSAM

In response to the European Parliament question, the Commission services asked Member States the following questions:

1) Is there any national legislation in your Member State that permits or mandates providers of (number-independent) interpersonal communications services to detect, report and/or remove child sexual abuse online?
2) Is there any national legislation in your Member State that permits or mandates other providers of electronic communications services to take any action with regard to child sexual abuse online?

   If you answered either of the two first questions with “Yes”, could you please share that legislation, ideally describing briefly its scope (i.e. which services are covered, what actions are permitted or imposed?, etc) and conditions of application?

Please find below the responses provided by Member States:

1) AT
Q1/2: No, there is no such national legislation in Austria.

2) BE
Q1: Belgian law does not regulate proactive measures by providers. However, when a provider has knowledge that his services are being used for illegal content (such as SCAM), it has the obligation to report this to the national authorities and block or delete access to the content. A provider can for example become aware of the illegal content when reported by its users, the police or trusted flaggers such as Child Focus.

CODE PENAL.

Art. 383bis.§ 1. Sans préjudice de l'application des articles 379 et 380, quiconque aura sans droit exposé, offert, vendu, loué, transmis, fourni, distribué, diffusé, ou mis à disposition, ou remis du matériel pédopornographique ou l'aura produit, importé ou fait importer, sera puni de la réclusion de cinq ans à dix ans et d'une amende de cinq cents euros à dix mille euros.
§ 2. Quiconque aura sciemment et sans droit acquis, possédé du matériel pédopornographique ou y aura, en connaissance de cause, accédé par le biais des technologies de l'information et de la communication, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent euros à mille euros.
§ 3. L'infraction visée sous le § 1er, sera punie (de la réclusion) de dix ans à quinze ans et d'une amende de cinq cents [euros] à cinquante mille [euros], si elle constitue un acte de participation à l'activité principale ou accessoire d'une association, et ce, que le coupable ait ou non la qualité de dirigeant.
§ 4. Pour l'application du présent article, on entend par "matériel pédopornographique" :
1° tout matériel représentant de manière visuelle, par quelque moyen que ce soit,

un mineur se livrant à un comportement sexuellement explicite, réel ou simulé, ou représentant les organes sexuels d'un mineur à des fins principalement sexuelles;
2° tout matériel représentant de manière visuelle, par quelque moyen que ce soit, une personne qui paraît être un mineur se livrant à un comportement sexuellement explicite, réel ou simulé, ou représentant les organes sexuels de cette personne, à des fins principalement sexuelles;
3° des images réalistes représentant un mineur qui n'existe pas, se livrant à un comportement sexuellement explicite, ou représentant les organes sexuels de ce mineur à des fins principalement sexuelles
§ 5. Les articles 382, 382ter, 382quater, 382quinquies et 389 s'appliquent aux infractions visées aux paragraphes 1er à 3.

Code de droit économique

Section 2. - Activité de stockage sous forme de copie temporaire de données

Art. XII.18. En cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire n'est pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, pour autant que chacune des conditions suivantes soit remplie :
1° le prestataire ne modifie pas l'information;
2° le prestataire se conforme aux conditions d'accès à l'information;
3° le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisée par les entreprises;
4° le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information;
5° le prestataire agit promptement pour retirer l'information qu'il a stockée ou pour rendre l'accès à celle-ci impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'une autorité administrative ou judiciaire a ordonné de retirer l'information ou de rendre l'accès à cette dernière impossible et pour autant qu'il agisse conformément à la procédure prévue à l'article XII.19, § 3.

Section 3. - Activité d'hébergement

Art. XII.19. [1 § 1er. En cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition :
1° qu'il n'ait pas une connaissance effective de l'activité ou de l'information illicite, ou, en ce qui concerne une action civile en réparation, qu'il n'ait pas connaissance de faits ou de circonstances laissant apparaître le caractère illicite de l'activité ou de

l'information; ou
2° qu'il agisse promptement, dès le moment où il a de telles connaissances, pour retirer les informations ou rendre l'accès à celles-ci impossible et pour autant qu'il agisse conformément à la procédure prévue au paragraphe 3.
§ 2. Le paragraphe 1er ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.
§ 3. Lorsque le prestataire a une connaissance effective d'une activité ou d'une information illicite, il les communique sur le champ au procureur du Roi qui prend les mesures utiles conformément à l'article 39bis du Code d'instruction criminelle.
Aussi longtemps que le procureur du Roi n'a pris aucune décision concernant le copiage, l'inaccessibilité et le retrait des documents stockés dans un système informatique, le prestataire peut uniquement prendre des mesures visant à empêcher l'accès aux informations.

Q2 : No, the Belgian law of 13 June 2005 concerning electronic communications does not include any provision is this regard.

3) BG

Q1: Currently in Bulgaria there is no national legislation that permits or mandates providers of (number-independent) interpersonal communications services to detect, report and/or remove child sexual abuse online.

With regard to national legislation **in preparation,** having in mind that NI-ECS providers will fall in the scope of the European Electronic Communications Code after 21 December 2020, we have planned to include them in the national legislation where we have transposed the requirements of Art. 15.1 of Directive 2002/58/EO (e-Privacy Directive) which mandates ECS providers to provide access to traffic data generated, processed or stored by them to law enforcement authorities for the purposes of national security and the prevention, investigation and prosecution of serious crimes. According to our criminal law, child sexual abuse online is a serious crime and therefore the competent law-enforcement authorities have the right to access relevant traffic data when working on such cases. In this regard, the national legislation should provide that there is no differentiated treatment of the providers depending on their category.

However, we had planned the measure before the Commission tabled the new dossier for a temporary derogation.

Currently, the planned national measures are subject to discussion in the national parliament. We will follow closely the debates on the dossier for derogation from the e-Privacy Directive before we take a final decision on our approach to NI-ECS.

Q2: See answers to the first question.

4) CY

Q1/Q2: The law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, law 91(i)/2014

which ratifies the EU Directive 2011/93/EE covers notice and takedown. According to the articles:

Under the article 11 (3) (a) of the law 91(i)/2014 the Internet service providers who offer services or access to the Internet within the territory of the Republic shall be obliged, as soon as they become aware or being informed of the existence of child pornography on any website, to take appropriate action immediately. Blocking access by internet users.
(b) Violation of the obligation referred to in paragraph (a) constitutes a criminal offense, punishable by imprisonment of not more than three (3) years or by a fine not exceeding one hundred and seventy thousand euros (€ 170,000) or by these two sentences.

There isn't an explicit legal basis obliging the providers to detect such material. The detection is limited to reports from the police, the Court and any other sources.

5) CZ
Q1: In this case, the Act no. 480/2004 Coll. – Act on certain information society services and on the amendment of certain acts can be applied.

Specifically § 5 – "The service provider's responsibility for storing the content of the information provided by the user"
(1) The service provider, which consists of storing the information provided by the user, is responsible for the content of the information stored at the request of the user, only (a) if in view of the subject of his activity and the circumstances and nature of the case, was aware that the content of the information stored or the user's conduct was unlawful, or (b) if he has demonstrably become aware of the unlawful nature of the content of the stored information or of the unlawful conduct of the user and has not immediately taken all steps that may be required of him to remove or make such information inaccessible.
(2) The service provider referred to in paragraph 1 is always responsible for the stored information content in case the direct or indirect decisive influence on the user's activity is concerned.

Q2: The § 7b) of the Act no. 141/1961 Coll. of the Criminal Procedure Code is used, "(2) If necessary to prevent the continuation or recurrence of criminal offenses, a person who holds or controls data stored in a computer system or on an information medium may be ordered to prevent the access of other persons. In general, the provider should act immediately in relation to the removal or inaccessibility of defective content as soon as it becomes aware of such content. If he is lax, he may face the risk of criminal prosecution.

6) DE
Q1: No
Q2: No

7) DK

Q1: There is no independent regulation in Denmark regarding social media platforms responsibility for the content on their platforms. However, social media platforms are – like other digital platforms – subject to the e-commerce directive.

Q2: The Danish government decided in November 2019 to establish a working group which is currently looking into possible initiatives and solutions regarding regulating the responsibility of social media platforms for illegal content on their platforms.

8) EE

Q1: No. However, we have different possibilities for voluntary cooperation between law enforcement and service providers regarding detecting, reporting and/or removing child sexual abuse online.

Q2: No. However, we have different possibilities for voluntary cooperation between law enforcement and service providers regarding detecting, reporting and/or removing child sexual abuse online.

9) EL

Q1: No

Q2: The existing legal framework (art. 18, Law 4267/2014) ensures a fast and flexible way of removing child pornography material. In particular, the Public Prosecutor to the Court of First Instance or to the Court of Appeal, if the case is pending before the Court of Appeal, can order the internet service provider in Greece to block access to any website of such content. This order of the Public Prosecutor, which must be specifically and fully reasoned, shall be notified to the Hellenic Telecommunications and Post Commission (EETT, the Greek NRA), which shall ensure the order's immediate execution (art. 18 Law 4267/2014).

In addition, we would like to mention that our legislative framework also provides for either the child himself/herself or those exercising parental responsibility to report the act to the competent police authorities and request the removal. The police cooperate with the Public Prosecutor, who shall, where appropriate, issue the abovementioned order. Furthermore, the child or the parents could also approach and make their report to relevant civil society organizations or use a special helpline, which offer mainly support and advice but, in view of the criminal nature of the act, these organizations should report the act to the competent Public Prosecutor or to the police in order to initiate the aforementioned procedure.

10) ES

Q1: IN FORCE: In the Spanish General Telecommuncations Law, there is only lawful Interception, which would be similar to reporting, but in any case with prior judicial authorization. But this is certainly not detection.
In the Information Society Services Law, there is the obligation to delete the domain name, but this is done by the assigning authority, not by any provider.

IN PREPARATION: What there is in Parliament now is a proposed Organic Law for the integral protection of children and adolescents against violence, which establishes

in Article 18 the duty to communicate this illicit content on the Internet, a generic duty that affects all individuals and legal entities:

Article 18. Obligation to communicate illegal content on the Internet. 1. Any natural or legal person who notices the existence of content available on the Internet which constitutes a form of violence against any child or adolescent is obliged to communicate it to the competent authority and, if the facts could constitute a crime, to the Security Forces, the Public Prosecutor's Office or the judicial authority. 2. Public Administrations shall guarantee the availability of accessible and secure channels for reporting the existence of such content. These channels may be managed by national reporting lines approved by international networks, always in collaboration with the Security Forces..

Artículo 18. Deber de comunicación de contenidos ilícitos en Internet. 1. Toda persona, física o jurídica, que advierta la existencia de contenidos disponibles en Internet que constituyan una forma de violencia contra cualquier niño, niña o adolescente, está obligada a comunicarlo a la autoridad competente y, si los hechos pudieran ser constitutivos de delito, a las Fuerzas y Cuerpos de Seguridad, al Ministerio Fiscal o a la autoridad judicial. 2. Las Administraciones Públicas deberán garantizar la disponibilidad de canales accesibles y seguros de denuncia de la existencia de tales contenidos. Estos canales podrán ser gestionados por líneas de denuncia nacionales homologadas por redes internacionales, siempre en colaboración con las Fuerzas y Cuerpos de Seguridad.

Q2: No

11) FI:
Q1: Not directly what comes to number-independent providers, see below in Q2.
Q2: In force: Act on the prohibition of child pornography (codes: HE 99/2006, 1068/2006).
It prohibits access to websites displaying child pornographic material and sets requirements for law enforcement authorities to maintain and update a list of such websites. In principle number-independent communications services do not administer access to certain websites, so this does not apply to them.

Draft: Draft Act on electronic communications services (code: HE 98/2020), 185 § - Parliamentary process underway - prohibition of access to information; according to which the court can order with subject to penalties a telecom service provider to prevent general access to information that is prohibited by law. The goal of this amendment is for law enforcement authorities to be able to have better access to illegal material for the purposes of preventing and investigating crimes. This applies to telecom service providers, who have the possibility to prohibit access to websites.

12) FR
Pending

13) HR

Q1: No
Q2: No

14) HU
Q1: There is no specific legal provision in Hungary allowing the detection, reporting or removing such online content.

Nevertheless, as from 21 December, according to a new provision of the Hungarian Electronic Communications Act, OTT-providers will be obliged to make users available (for free) a content-filtering software for the protection of minors.

The Hungarian Electronic Communications Act provides (currently in force):
Section 149/A para 1 - Providers of internet access shall make available on their website an easy-to-install and user-friendly software designed for the protection of minors, in Hungarian (hereinafter referred to as "content-filtering software"), that can be downloaded and used free of charge
para 2 - The Internet Round-table Conference for the Protection of Children (hereinafter referred to as "Round-table Conference") shall make out and publish recommendations for providers of internet access so as to facilitate the development and selection of content-filtering software that meets the requirements set out in Subsection (1). The Round-table Conference shall encourage service providers to coordinated their efforts in developing their own self-regulatory policies relating to content-filtering software, and shall provide assistance to that end.

Q2: In Hungary, the Electronic Communications Act has a stipulation regarding the cooperation between the NRA and ECS providers with a view to blocking access to websites containing child pornography.

Section 159/D para 1 - Electronic communications service providers of access and providers of browsing and caching services shall be entitled to render electronic information containing images of child pornography contained in the list maintained by the International Criminal Police Organization (INTERPOL) inaccessible.

The INTERPOL establishes a so-called "worst of" list of domain names with the most serious child pornography content based on a pre-established definition. This allows service providers – voluntary - to block these websites without examining the content.

15) IE
Q1/Q2: The short answer to both questions as regards enacted legislation is no.

Ireland currently applies a voluntary approach to this area where: 1) An Garda Síochána have a good working relationship and clear channels of communications with HSPs in Ireland; and 2) as embodied by the Irish branch of the INHOPE network of international reporting hotlines, and our work in DoJ to update the hotline's approach to this area and to encourage increased levels of corporate membership and collaboration amongst members in same.

Section 9 Offences by bodies corporate of the Child Trafficking and Pornography Act, 1998 is possibly the closest Irish legislation comes to such a provision in terms of the nature of a body corporate's role/responsibility in this area.

Of particular note here is the proposed Online Safety and Media Regulation Bill which defines a category of harmful content as "material which it is a criminal offence to disseminate" and includes forms of such content defined in EU law. This Bill seeks to establish a regulatory framework to tackle the spread and amplification of certain defined categories of harmful online content through binding online safety codes as overseen by an Online Safety Commissioner as part of a wider Media Commission.

The extent to which an online safety code, as applicable to illegal content, would encompass the specific duties as described in the below questions is to be determined.

16) IT

Q1/Q2: Italy approved a national legislation on this issue in 2006 (L 6/2/2006, n. 38 concerning the fight against sexual exploitation of children and child pornography, including through the Internet).

As refers to your questions, please consider that the main obligations of providers of number-independent interpersonal communication services are set our under art. 19 and 20 of the above mentioned national Law (L. 6/2/2006 nr. 38).

Art. 19 amends Law 3/08/98 nr. 269 and introduces three new provisions (namely art. 14 ter, 14 quarter and 14 quinquies) respectively governing the cases of "Obligations for providers of information services delivered through electronic communications networks" (Art. 14 ter) , "Use of technical tools to prevent access to websites that disseminate child pornography material" (Art. 14 quarter) and "Financial measures to combat the marketing of child pornography" (Art. 14 quinquies).

Furthermore the mentioned L. 2006/38 created also the so called "National Center for the fight against child pornography on the INTERNET network (web)" (hereinafter referred to as the "Center"). The Center is established within the Ministry of the Interior and it is tasked of collecting all reports from Leas (also from other countries) and from public and private entities involved in the fight against child pornography, regarding websites that disseminate material concerning the sexual exploitation of minors as well as managers and beneficiaries of related payments.

According to art 14 ter:

- ISPs are obliged to report to the "National Center", if they become aware of them, the companies or entities (persons) who, for any reason, disseminate, distribute or trade, even electronically, child pornography material
- ISPs are also obliged to communicate without delay to the Center, upon request, any information relating to contracts with such companies or entities.
- The service providers must keep the material for at least forty-five days.

- Unless the fact constitutes a crime, the violation of the mentioned obligations entails a pecuniary administrative sanction from € 50,000 to € 250,000.
- In the event of violation of the obligations referred to in paragraph 1, the reduced payment referred to in Article 16 of Law no. 689.

According to art 14 quater:

- ISPs, in order to prevent access to the websites indicated by the Center, are obliged to use the filtering tools and the related technological solutions that comply with the requirements identified by Decree of the Minister of Communications, in agreement with the Minister for Innovation and Technologies and after consulting the most representative associations of the INTERNET network connectivity providers. The same decree also indicates the term within which the providers of connectivity to the INTERNET network must equip themselves with filtering tools.
- The violation of the obligations above mentioned is punished with a pecuniary administrative sanction from € 50,000 to € 250,000. The Ministry of Communications provides for the imposition of the sanction.

17) LT

Q1: There are general provisions (in the Law on Education) related to combat bullying in the cyberspace. Users can inform about such facts using a platform *www.draugiskasinternetas.lt (hotline and helpline numbers are provided as well).* The information which is classified as "prohibited" is defined in the Law on Child Protection from Negative Information Influence and encompass different type of harassment/ bullying, such as based on racial, gender, origin, disability, sex, language, religion and various other grounds or, information which is related to CSA.

NIICS service providers are not in the scope.

Q2: No. NIICS providers are not in the scope under Law on Education. On the other hand, the Law on Information Society Services, have certain provisions related to data retention information blocking/ deletion, but the provisions target hosting providers, not the NIICS.

18) LU
Q1: No
Q2: No
The above is based on a preliminary assessment.

19) LV
Q1: There is no law that impose an obligation on providers of number-independent interpersonal communications services to take any actions. If illegal / criminal activities are detected, they should be reported immediately to the relevant law-enforcement authorities, but the law does not oblige to search / perform data supervision.

Regarding the first question please be informed that according to the Law on Information Society Services (https://likumi.lv/ta/en/en/id/96619-law-on-information-society-services) if intermediary service provider (*a provider of the information society service, which ensures the transmission of information in an electronic communication network, access to an electronic communication network or the storage of information*) detects forbidden content, it informs proper authorities immediately (Article 11). Nevertheless an intermediary service provider does not have a duty to supervise the information, which the provider transmits or stores, as well as to actively search for the facts and conditions, which indicate possible violations of the law (Article 11(2).). Authorities can demand that the intermediary services provider do everything necessary to eliminate the breach (Article 13).

The Law on Pornography Restrictions (https://likumi.lv/ta/en/en/id/157638-law-on-pornography-restrictions) defines the "child pornography" in Article 1(2). Article 4(1) sets out a ban on child pornography as such, while Article 4(2) forbids to involve children in creation of such materials.

Q2: Regarding the second question please be informed that according to Article 34(2)11 of the Electronic Communications Law (https://likumi.lv/ta/en/en/id/96611-electronic-communications-law) similar rules apply to the other electronic communications merchants according to points 18. to 21 of the General Authorisation Regulations in the Field of Electronic Communications (https://likumi.lv/ta/en/en/id/303972-general-authorisation-regulations-in-the-field-of-electronic-communications).

In particular point 18 prescribes general rule that "the electronic communications merchant shall conform to the restrictions of the transmission of the information of illegal content specified in the laws and regulations". Point 19 prescribes that "the electronic communications merchant shall not encourage access to the information the distribution of which on the Internet is prohibited in accordance with the laws and regulations. The point 21 prescribes that "the electronic communications merchant does not have an obligation to supervise the content of information transmitted thereby,(..), as well as does not have an obligation to search for the facts and circumstances indicating to the transmission of information of illegal content" which is similar rule as in Article 11(2) of Law on Information Society Services.

20) MT

Pending

21) NL

Q1: No

Q2: Yes

NL has a notice-and-take-down procedure, which is laid down in Article 125p of the Code of Criminal Procedure (see attachment). The NTD also applies to CSAM.

The said provision is a part of the so-called Computer Crime III Act, which also criminalises grooming of children. For more information please follow this link https://www.government.nl/latest/news/2019/02/28/new-law-to-help-fight-computer-crime .

Aside from criminal law, civil law also offers avenues. Article 196c of Book 6 of the NL Civil Code. Said provision lays down the exemptions for liability when hosting unlawful content.

22) PL

Q1: No

Q2: No

23) PT

Q1: There´s no national legislation that permits or mandates providers of (number-independent) interpersonal communications services (NIIC) services to detect, report and/or remove child sexual abuse online

According to the Electronic Communications Act in force in Portugal (Law 5/2004, of 10th of February), electronic communication providers have to comply with the communication´s confidentiality principle, meaning that it is forbidden to have access to any content (scanning or screening).

Electronic communication providers can only access communication's content under law enforcement authorities, for a limited period of time, regarding a single out suspect(s) of an illegal activity and only for criminal investigation purposes (which means that the envisaged conduct has to be considered a criminal offense under the Portuguese law).

From the criminal point of view, regarding CSAM, Portugal´s Penal Code follow the definitions of Directive 2011/93/EU of the European Parliament and of the Council of 13th December (on combating the sexual abuse and sexual exploitation of children and child pornography).

The recently updated eCommerce Portuguese Law (Act 7/2004 of 17 January 2004 transposing into national law 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) provides a (new) obligation to the intermediary providers of networked services (not electronic communication service providers) to immediately inform the Public Prosecutor's Office of the detection of content made available by means of the services they provide whenever the provision of such content, or access to it, may constitute a crime, in particular a crime of pornography of minors or a crime of discrimination and incitement to hatred and violence (Article 19-A).

According to Article 19-B, they also have a blocking duty: within 48 hours, they must ensure the blocking of sites identified as containing pornography of minors or related material through a transparent procedure with appropriate safeguards, in particular by ensuring that the restriction is limited to what is necessary and proportionate and that users are informed of the reason for the restriction.

Websites identified as containing pornography of minors or related material shall be considered to be all those included in the lists drawn up for that purpose by the national and international bodies responsible for preventing and combating crime in accordance with the following paragraph.

The blocking may be challenged before the competent judge, in general terms (Article 19-B (4)).

Omission of the information provided for in Article 19-A or the blocking provided for in Article 19-B constitutes an offence:

a) in the case of intent, with a fine of (euro) 5000 to (euro) 100 000;

b) in the case of negligence, with a fine of (euro) 2500 to (euro) 50 000 (Article 37(4) c.).

The practice of an infringement by a legal person increases the maximum and minimum limits of the fine by one third (Article 37(6)).

There is the possibility of imposing ancillary sanctions (Article 38) and interim measures (Article 39).

Q2: There´s no national legislation that permits or mandates other providers of electronic communications services to take any action with regard to child sexual abuse online.

24) RO

Q1: Law No. 365/2002 on e-commerce.
”(1) The service providers are bound to notify the competent public authorities right away, about activities that seem illegal carried out by the recipients of their services or about information supplied by these ones that seem illegal.

Q2: Law No. 365/2002 on e-commerce.
(2) The service providers are bound to interrupt, temporarily or permanently, the transmission into a communication network or the storage information supplied by a recipient of the respective service, especially by eliminating the information or by blocking the access to it, the access to a communication network or the supply of any other information society service, if these measures were required by a public authority, ex-officio or at the receipt of a claim or complaint from any person.
Romanian police, under the law, require Internet service providers from Romania to remove illegal material with minors after checking them according to the specific procedure. In cases where it appears that the images are hosted by providers from other countries, we inform the judicial authorities in those states. Author of the reports (eg public, ISP, industry, hotline “safernet.ro”)

Competent authorities which may authorize for enclosure and eliminate illegal material involving minors are public administration authorities or, where appropriate, the court, whose jurisdiction in question is determined by the legal provision in force, applicable in each case. The private sector is responsible for implementing the measures taken by the competent authorities or by blocking or removing illegal content.

Service providers are not liable for content if they provide services, who has leased or used the service is responsible for the content, but if the service provider is aware of illegal content, it should eliminate it and report it to competent authorities for investigation."

25) SE

Q1: No, there is no legislation in force in Sweden providing a legal basis for interpersonal (number-independent) communication services to detect, report and/or remove child sexual abuse online. Sweden welcomes the proposal to offer a legal basis for detection, report and/or removal of child sexual abuse for these service providers.

Q2: The blocking, or rather re-direction, of websites with child sexual abuse content is since 2005 carried out in voluntary cooperation between the Police and the Internet Service Providers (ISP). 85-90 % of subscribers have been covered by a handful of the major ISP's, but the figure is currently unclear.

The cooperation operates in the following way: The Police receives information on child pornographic websites from different channels such as Europol, Interpol, child right organisations or the general public. Information is also collected by the Police in its daily work on acting against child sexual abuse online.

The information is verified and then shared with the Internet Service Providers who make the technical arrangements for blocking at the level of the end user on the basis of the contractual relation between the subscribers and the ISP. This means that anyone trying to access the website in question, instead will see a message (see annex) saying that the site is blocked due to its child pornographic content. In other words, websites with child pornographic content will be blocked and made not accessible in Sweden regardless of whether the site is located within or outside the EU.

Consequently, Sweden is in favour of including the ISP's within the scope of the upcoming proposal on this issue, such an inclusion would provide a clear legal basis as well as clear and precise conditions for taking action against child sexual abuse online also by the ISP's.

26) SI

Q1: No

Q2: No

27) SK

Q1: Not aware of this kind of specific legislation

Q2: -