COMPROMISE AMs - BATCH VI (AMs 879 - 1050)

CSA
(rapporteur: Javier ZARZALEJOS)

Batch endorsed SM 24/10/2023
In red changes agreed SM 24/10/2023

Article 7 - Issuance of detection orders

Covers: AMs 107 (rapp), 108 (rapp), 109 (rapp), 110 (rapp), 111 (rapp), 113 (rapp), 114 (rapp), 115 (rapp), 116 (rapp), 117 (rapp), 121 (rapp), 123 (rapp), 124 (rapp), 125 (rapp), 126 (rapp), 127 (rapp), partially 128 (rapp), 143 (rapp), partially 896 (ECR), partially 898 (EPP), 902 (Greens), 905 (ECR), 908 (Greens), partially 909 (S&D), partially 910 (S&D), 911 (Greens), 924 partially (Greens), 925 (ChildIntergroup), 928 partially (ChildInterg), 935 (RE), partially 939 (Greens), partially 942 (Greens), 944 partially (S&D), 945 partially (S&D), 946 partially (ECR), 947 partially (Greens), 950 (EPP), 951 (RE), partially 952 (S&D), partially 953 (S&D), 954 (Greens), 955 (EPP), 956 (ECR), 958 (Greens), partially 959 (S&D), partially 960 (S&D), 961 (ECR), partially 962 (S&D), 963 (ECR), 964 (EPP), 965 (Greens), 967 (RE), 968 partially (S&D), 969 (ECR), 972 (ECR), 974 (Greens), 975 (EPP), 976 (ECR), 978 (ECR), 980 (ECR), 982 (S&D), 983 (ECR), 984 (S&D), 985 (ECR), 986 (S&D), 988 (Greens), 989 (ECR), 1014 (ID), partially 1017 (EPP), partially 1019 (S&D), 1024 partially (S&D), 1030 partially (Renew), 1031 partially (ChildrenIntergroup), 1036 (ECR), 1038 (Greens), 1042 (Greens), partially 1046 (S&D), partially 1047 (S&D), part. 132 (IMCO), part. 133 (IMCO), 134 (IMCO), part. 153 (IMCO), part. 135 (IMCO), part. 136 (IMCO), part. 140 (IMCO), part. 143 (IMCO), 150 (IMCO), part. 144 (IMCO), 147 (IMCO), part. 166 (IMCO), 167 (IMCO), 169 (IMCO), 171 (IMCO), 172 (IMCO).

Fall: AMs 112 (rapp), 118 (rapp), 119 (rapp), 120 (rapp), 122 (rapp), 129 (rapp) 879 (ECR), 880 (ECR), 881 (Left), 882 (EPP), 883 (S&D), 884 (S&D), 885 (ECR), 886 (S&D), 887 (S&D), 888 (EPP), 889 (Greens), 890 (RE), 891 (ECR), 892 (RE), 893 (EPP), 894 (RE), 895 (RE), 899 (ECR), 900 (EPP), 901 (S&D), 903 (EPP), 904 (S&D), 906 (ECR), 907 (EPP), 912 (ECR), 913 (S&D), 914 (S&D), 915 (S&D), 916 (Greens), 917 (S&D), 918 (S&D), 919 (S&D), 920 (S&D), 921 (S&D), 922 (ECR), 923 (S&D), 926 (S&D), 927 (ECR), 929 (Greens), 930 (S&D), 931 (ECR), 932 (S&D), 933 (Greens), 934 (EPP), 936 (ECR), 937 (S&D), 938 (EPP), 940 (ECR), 941 (S&D), 943 (ECR), 948 (ECR), 949 (ECR), 957 (ECR), 966 (S&D), 977 (S&D), 979 (S&D), 981 (S&D), 987 (S&D), 990 (S&D), 991 (S&D), 992 (ECR), 993 (S&D), 994 (Greens), 995 (S&D), 996 (ECR), 997 (EPP), 998 (ECR), 999 (ECR), 1000 (EPP), 1001 (S&D), 1002 (ECR), 1003 (Greens), 1004 (S&D), 1005 (S&D), 1006 (S&D), 1007 (Greens), 1008 (ECR), 1009 (EPP), 1010 (S&D), 1011 (ECR), 1012 (S&D), 1013 (S&D), 1015 (ECR), 1016 (EPP), 1018 (EPP), 1020 (Greens), 1021 (ECR), 1022 (S&D), 1023 (Renew), 1025 (Renew), 1026 (S&D), 1027 (Greens), 1028 (S&D), 1029 (S&D), 1032 (Greens), 1033 (Greens), 1034 (ECR), 1035 (Renew), 1037 (EPP), 1039 (Greens), 1040 (EPP), 1041 (S&D), 1043 (S&D), 1044 (EPP), 1045 (S&D), 1048 (S&D), 1049 (Renew), 1050 (Renew), 137 (IMCO), 138 (IMCO), 139 (IMCO), 141 (IMCO), 142
Protection of encryption covered IN Article 10 (3) (da): AM 897 (Greens, ECR, SD, RE), 970 (S&D), 971 (ECR), 973 (ECR)

Article 7
Issuance of detection orders

1. **As a last resort** (part. 905 ECR) **after all the measures in Article 3, 4 and 5 have been exhausted** (AM 107 rapp, 972 ECR, part. 132 IMCO, part. 896 ECR,), the Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State (part. 886 S&D, part. 887 S&D, part. 888 EPP, part. 889 Greens, part. 890 RE, 892 RE, partially 893 EPP, 132 part. IMCO) to issue a detection order requiring a provider of hosting services or a provider of number-independent (part. 886 S&D, part. 887 S&D, part. 889 Greens, 132 part IMCO) interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect and prevent (AM 894 RE) online child sexual abuse material on a specific service.

The detection order shall be targeted (part. 888 EPP, part. 893 EPP) and specified and limited to an identifiable part or component of the service, such as a specific channel of communication, or to individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication, in respect of whom there are objective evidence reasonable grounds of suspicion that reveal for a link, even an indirect or remote one, with online child sexual abuse material as defined in Article 2. (part. 900 EPP)

The content of interpersonal communications to which end-to-end encryption is, has been or will be applied shall not be subject to the measures specified in Article 10. (partially 170 IMCO, partially 897 (Greens, ECR, SD, RE))

Detection orders shall be addressed to the service provider acting as controller in accordance with Regulation (EU) 2016/679. (part. 133 IMCO, part. 896 ECR) By way of exception, the detection order may be directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, where:

(a) the controller cannot be identified despite reasonable efforts on the part of the issuing authority; or

(b) addressing the controller might be detrimental to an ongoing investigation

2. **Based on a reasoned justification** (AM 954 Greens), the Coordinating Authority of establishment shall, before requesting (part 108 rapp) the issuance of the detection order carry out the investigations (AM 902 Greens) and assessments necessary to determine whether the conditions of paragraph 4 have been met and the competent
judicial authority or independent administrative authority shall issue the detection order where it considers that all (AM 134 IMCO) the following conditions are simultaneously met (AM 108 rapp, 950 EPP, AM 951 RE, partially 952 SD, partially 953 SD):

(a) there is are reasonable grounds of suspicion on individual users, or on a specific group of users, either as such or as subscribers to a specific channel of communication, in respect of whom there is a link, even an indirect one, with online–child sexual abuse material as defined in Article 2. there is objective substantive (AM partially 959 SD, partially 960 SD) evidence that reveal a link, at least an indirect one, of a significant risk of (961 ECR) the service being used for the purpose of online child sexual abuse material, within the meaning of paragraphs 5, 6 and 7, as applicable; (AM 109 rapp, part. 958 Greens, part. 959 S&D, part. 960 S&D). Reasonable grounds of suspicion objective elements evidence are those resulting from any information reliable and legally acquired that constitute reasonable grounds to suggest that individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication might have a link, even an indirect or remote one, with online–child sexual abuse material.

(b) the mitigation measures put in place by the provider have insufficient material impact on limiting the identified risk (AM part. 153 IMCO) are not considered effective and proportionate to the risk of the misuse of the service offered or the service provider fails to to put in place reasonable and proportionate mitigation measures set out in this Regulation. (AM 110 rapp, 967 RE, 972 ECR)

(c) issuing the detection order is necessary and proportionate and outweighs (AM 905 ECR, partially 962 S&D, 965 Greens) negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties (AM 111 rapp, part. 905 ECR), and without jeopardising the security of communications (AM partially 968 SD, part. 969 ECR, 147 IMCO)

To that end, it may, where appropriate, require the provider to submit the necessary information, additional to the report and the further information referred to in Article 5(1) and (3), respectively, within a reasonable time period set by that Coordinating Authority, or request the EU Centre, another public authority or relevant experts or entities to provide the necessary additional information.

3. Where the Coordinating Authority of establishment takes the preliminary (AM 908 Greens, part. 135 IMCO) view that all the conditions of paragraph 4 2 (AM 113 rapp) have been met, it shall:

(a) establish a draft request to the competent judicial authority of the Member State that designated it or independent administrative authority (AM partially 909 SD, partially 910 SD, part. 136 IMCO) for the issuance of a detection order, specifying the factual and legal grounds upon which the request is based (AM 911 Greens, part. 136 IMCO) and the duration of the order, as well as (part. 136 IMCO), the main elements of the content of the detection order it intends to request and the reasons for requesting it;
(b) submit the draft request to the provider and the EU Centre,

(c) afford the provider an opportunity to comment on the draft request, within a reasonable time period set by that Coordinating Authority;

(d) invite the EU Centre, and in particular its Technology Committee (AM 925 SD, RE, EPP), to provide its opinion on the draft request, within a time period of four weeks from the date of receiving the draft request.

Where, having regard to the comments of the provider and the opinion of the EU Centre, that Coordinating Authority continues to be of the view that the conditions of paragraph 42 have been met and prior to requesting the competent judicial authority the issuance of the detection order (AM partially 924 Greens), it shall re-submit the draft request, adjusted where appropriate, to the provider. In that case, request the provider shall to do all of the following, within a reasonable time period set by that Coordinating Authority, which cannot exceed four weeks: (AM 114 rapp)

(a) draft an implementation plan setting out the measures it envisages taking to execute the intended detection order, including detailed information regarding the envisaged technologies and their technical feasibility (AM 984 S&D) and safeguards and if any, the negative impacts and safeguards on the rights of all parties involved (part. 140 IMCO). The provider may consult the EU Centre, and in particular its Technology Committee, to obtain support in identifying appropriate measures in this respect (AM partially 928 SD, RE, EPP);

(b) where the draft implementation plan concerns the use of any specific technology for the purpose of complying with an intended detection order concerning new child sexual abuse material or solicitation of children other than the renewal of a previously issued detection order without any substantive changes, conduct a data protection impact assessment and a prior consultation procedure as referred to in Articles 35 and 36 of Regulation (EU) 2016/679, respectively, in relation to the measures set out in the implementation plan;

(c) where point (b) applies, or where the conditions of Articles 35 and 36 of Regulation (EU) 2016/679 are met, adjust the draft implementation plan, where necessary in view of the outcome of the data protection impact assessment and in order to take due into account of (based on AM 939 Greens) the opinion of the data protection authority provided in response to the prior consultation;

(d) submit to that Coordinating Authority the implementation plan, where applicable attaching the opinion of the competent data protection authority and specifying how the implementation plan has been adjusted in view to take due account (based on AM 942 Greens, part. 143 IMCO) of the outcome of the data protection impact assessment and of that opinion.

Where, having regard to the implementation plan of the provider and the opinion of the data protection authority and, where applicable, the opinion issued in accordance with article 5 (4c) (121 rapp, 986 S&D, 150 IMCO), that Coordinating
Authority continues to be of the view that the conditions of paragraph 42 (AM 116 rapp) have been met, it shall submit the request for the issuance of the detection order, adjusted where appropriate, to the competent judicial authority or independent administrative authority (AM partially 944 SD, partially 945 SD, partially 946 ECR, partially 947 Greens, part. 144 IMCO). It shall attach the implementation plan of the provider and the opinions of the EU Centre and the data protection authority to that request.

Where that Coordinating Authority substantially deviates from the opinion of the EU Centre or the data protection authority, it shall inform the EU Centre or the data protection authority and the Commission thereof, specifying the points at which it deviated and the main reasons for the deviation. (AM 122 rapp, 990 S&D, 991 partially S&D)

4. The Coordinating Authority of establishment shall request the issuance of the detection order, and the competent judicial authority or independent administrative authority shall issue the detection order where it considers that the following conditions are met: (AM 117 rapp)

(a) there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5, 6 and 7, as applicable; (AM 955 EPP, 956 ECR)

(b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties. (AM 963 ECR, 964 EPP)

When assessing whether the conditions of the first subparagraph have been met, account shall be taken of all relevant facts and circumstances of the case at hand, in particular: (AM 974 Greens, 975 EPP, 976 ECR)

(a) the risk assessment conducted or updated and any mitigation measures taken by the provider pursuant to Articles 3 and 4, including any mitigation measures introduced, reviewed, discontinued or expanded pursuant to Article 5(4) where applicable; (AM 978 ECR)

(b) any additional information obtained pursuant to paragraph 2 or any other relevant information available to it, in particular regarding the use, design and operation of the service, regarding the provider’s financial and technological capabilities and size and regarding the potential consequences of the measures to be taken to execute the detection order for all other parties affected; (AM 980 ECR)

(c) the views and the implementation plan of the provider submitted in accordance with paragraph 3; (AM 982 S&D, 983 ECR)

(d) the opinions of the EU Centre and of the data protection authority submitted in accordance with paragraph 3. (AM 985 ECR)
As regards the second subparagraph, point (d), where that Coordinating Authority substantially deviates from the opinion of the EU Centre, it shall inform the EU Centre and the Commission thereof, specifying the points at which it deviated and the main reasons for the deviation. (AM 988 Greens, 989 ECR)

5. As regards detection orders concerning the dissemination of known child sexual abuse material, the significant risk objective evidence reasonable grounds of suspicion referred to in paragraph 4, first subparagraph, point (a), (AM 123 rapp) shall be deemed to exist where the following conditions are met:

(a) it is likely that, despite any the mitigation measures that the provider may have has (124 rapp) taken or will take, have insufficient material impact on limiting the systemic risk and the service is being used by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication, to an appreciable extent, for the dissemination of known child sexual abuse material; (based on AM 153 IMCO)

(b) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication and to an appreciable extent for the dissemination of known child sexual abuse material. (based on AM 154 IMCO)

6. As regards detection orders concerning the dissemination of new child sexual abuse material, the significant risk reasonable grounds of suspicion referred to in paragraph 4, first subparagraph, point (a), (AM 125 rapp) shall be deemed to exist where the following conditions are met:

(a) it is likely that, despite any the mitigation measures that the provider may have has (124 rapp) taken or will take, have insufficient material impact on limiting the systemic risk and the service is being used by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication, to an appreciable extent, for the dissemination of new child sexual abuse material;

(b) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication and to an appreciable extent for the dissemination of new child sexual abuse material.

(c) for services other than those enabling the live transmission of pornographic performances as defined in Article 2, point (e), of Directive 2011/93/EU:

(1) a detection order concerning the dissemination of known child sexual abuse material has been issued in respect of the service;
(2) the provider submitted a significant number of reports concerning known child sexual abuse material, detected through the measures taken to execute the detection order referred to in Article 12.

7. As regards detection orders concerning the solicitation of children, the significant risk objective evidence referred to in paragraph 4, first subparagraph, point (a), (AM 126 rapp) shall be deemed to exist where the following conditions are met:

(a) the provider qualifies as a provider of interpersonal communication services;

(b) it is likely that, despite any mitigation measures that the provider may have taken or will take, the service is used, to an appreciable extent, for the solicitation of children;

(c) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent, for the solicitation of children.

The detection orders concerning the solicitation of children shall apply only to interpersonal communications between where one of the users is a child user and an adult. (AM 127 rapp, 1014 ID)

8. The Coordinating Authority of establishment when requesting the issuance of detection orders, and the competent judicial or independent administrative authority (part. 166 IMCO) when issuing the detection order, shall in accordance with Article 8 of Regulation (EU) 2022/2065 (AM part 128 rapp, part. 1017 EPP, 1019 S&D) target and specify it in such a manner that the negative consequences referred to in paragraph 2, first subparagraph, point (b), remain limited to what is strictly necessary, justifiable and proportionate (AM part 128 rapp, part. 1017 EPP, part. 1019 S&D) to effectively target individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication address the significant risk as referred to in point (a) thereof, while not jeopardising the security of communications (part. 166 IMCO, partially 1024 SD); and, where possible, limit the detection order to an identifiable part or component of a service, such as a specific channel of communication or a specific group of users identified with particularity for which the significant risk has been identified.

To that end aim (167 IMCO), they shall take into account all relevant parameters, including the availability of sufficiently reliable detection technologies in that they limit to the maximum extent possible, in accordance with the state of the art in the industry (rapp proposal), the rate of errors regarding the detection, and their suitability and effectiveness for achieving the objectives of this Regulation, as well as the impact of the measures on the rights of the users affected, and require the taking of the least intrusive measures, in accordance with Article 10, from among several equally effective measures.

In particular, they shall ensure that:
(a) where the objective evidence referred to in paragraph 2 that risk is limited to an identifiable part or component of a service, the required measures are only applied in respect of that part or component;

(b) where necessary, in particular to limit such negative consequences, effective and proportionate safeguards additional to those listed in Article 10(4), (5) and (6) are provided for;

(c) subject to paragraph 9, the period of application remains limited to what is strictly necessary and proportionate (169 IMCO);

9. The competent judicial authority or independent administrative authority (AM 1036 ECR, 1038 Greens, 171 IMCO) shall specify in the detection order the period during which it applies, indicating the start date and the end date.

The start date shall be set taking into account the time reasonably required for the provider to take the necessary measures to prepare the execution of the detection order. It shall not be earlier than three months from the date at which the provider received the detection order and not be later than 12 months from that date.

The period of application of detection orders concerning the dissemination of known or new child sexual abuse material shall be proportionate, taking all relevant factor into account, and (1042 Greens, 172 IMCO) not exceed 24 months and that of detection orders concerning the solicitation of children shall not exceed 12 months.

10. Detections orders shall contain information about the right to appeal to a court of law according to the national legislation. (Rapp compromise following AM 1047 S&D)

Recital 20 to 23 - Article 7

Recital 20

Covers: AMs 13 (Rap.), part. 353 (EPP), part. 354 (ECR), part. 357 (S&D), part. 26 IMCO (**In recital 26: 356 EPP)

Fall: 352 (The Left), 355 (Greens), 359 (S&D), 360 (S&D), 361 (S&D)

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when the provider refuses to cooperate by putting in place the mitigating measures aimed (AM 13 rapp, part. 353 (EPP), part. 354 ECR) are deemed insufficient to limit the risk of misuse of a certain service for the purpose of online child sexual abuse, the Coordinating Authorities designated by Member States under this Regulation should be empowered to request, as a measure of last resort (AM 13 rapp, part. 353 EPP, part. 354 (ECR), part. 26 IMCO), the issuance of detection orders. In order to avoid any undue interference with fundamental rights and to ensure proportionality, that power should be subject to a carefully balanced set of limits and
safeguards. For instance, considering that child sexual abuse material tends to be disseminated through hosting services and publicly available number-independent (AM part. 357 S&D, part. 26 IMCO) interpersonal communications services, and that solicitation of children mostly takes place in publicly number-independent available interpersonal communications services, it should only be possible to address detection orders to providers of such services. As a matter of principle, detection orders shall be addressed to the service provider acting as a controller. However, in some circumstances, determining whether a service provider has the role of controller or processor can prove particularly challenging or addressing the controller could be detrimental to an ongoing investigation. Consequently, as an exception, it should be possible to address a detection order directly to the service provider that stores or otherwise processes the data.

Recital 21

Covers: AMs 14 (Rapp), partially 363 (Greens), partially 364 (S&D), Fall: 362 (The Left), 365 (EPP), 366 ID, 27 (IMCO)

(21) Furthermore, as parts of those limits and safeguards, detection orders should only be issued by a judicial authority and only (AM part. 364 S&D) after a diligent and objective assessment leading to the finding of reasonable grounds of suspicion for a link, at least an indirect one, of the a significant risk of the specific service concerned being misused by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication for a given type of online-child sexual abuse material covered by this Regulation. Reasonable grounds are those resulting from any information reliable and legally acquired that suggest that individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication might have a link, even an indirect or remote one, with online-child sexual abuse material. A link with child sexual abuse material should be deemed to exist where on the basis of objective evidence there is a reasonable suspicion that such material will be detected in the use of a service by a user. Where a channel is operated specifically for the purpose of distributing child sexual abuse material, the subscribers to that channel should be considered linked to child sexual abuse material. Conduct which is legal according to Directive 2011/92/EU or national law transposing it should not be deemed a reasonable ground of suspicion. For conducting such assessment a fluent dialogue must be established between the Coordinating Authority and the provider. In order to achieve that aim it should be possible for the Coordinating Authority to request additional information to the EU Centre, the competent data protection authorities or another public authority or entities. (AM 14 Rap.) One of the elements to be taken into account in this regard is the likelihood that the service is used to an appreciable extent, that is, beyond isolated and relatively rare instances, for such abuse. The criteria should vary so as to account of the different characteristics of the various types of online child sexual abuse at stake as well as the likelihood that the material could be rapidly disseminated (AM 366 ID) and of the different characteristics of the
services used to engage in such abuse, as well as the related different degree of intrusiveness of the measures to be taken to execute the detection order. (partially 363 Greens)

(21a) The definition of child sexual abuse material provided in article 2 has to be interpreted taking into account Directive 2011/93/EU. Therefore, personal face-to-face communication between consenting peers as well as children over the age of sexual consent and their partners are out of the scope of the definition insofar those images does not involve any abuse or exploitation or payment or remuneration for pornographic performance and the images have not been disseminated without the consent of the parties involved. Likewise, images produced for medical or scientific purposes, strictly verifiable as such, will remain out of the scope of definition of child sexual abuse material.

Recital 22
Covers: AMs part. 368 (S&D), part 369 (Greens), 370 (RE), part. 28 (IMCO),
Fall: AMs 367 (The Left), 23 (FEMM)

(22) However, the finding of such objective evidence (AM part. 368 S&D part 369 Greens), that constitute reasonable grounds to suggest that individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication might have a link, even an indirect or remote one, with online child sexual abuse material (AM part. 368 S&D) a significant risk should in itself be insufficient to justify the issuance of a detection order, given that in such a case the order might lead to disproportionate negative consequences for the rights and legitimate interests of other affected parties, in particular for the exercise of users’ fundamental rights. Therefore, it should be ensured that detection orders can be issued only after the Coordinating Authorities and the competent judicial or independent administrative authority (AM part. 369 Greens, 370 RE, part. 28 IMCO) having objectively and diligently assessed, identified and weighted, on a case-by-case basis, not only the likelihood and seriousness of the potential consequences of the service being misused for the type of online child sexual abuse material at issue, but also the likelihood and seriousness of any potential negative consequences for other parties affected, including the users of the service (AM part. 28 IMCO). With a view to avoiding the imposition of excessive burdens, the assessment should also take account of the financial and technological capabilities and size of the provider concerned.

Recital 23
Covers: AMs partially 15 (Rap.), part. 372 (Greens), partially 373 (EPP),
Falls: AMs 371 (The Left), 30 (IMCO), 31 (IMCO), 374 (ECR), part. 29 (IMCO)
In addition, to avoid undue interference with fundamental rights and ensure proportionality, when it is established that those requirements have been met and a detection order is to be issued, it should still be ensured that the detection order is limited in time specified (AM partially 15 Rapp., part. 372 Greens, partially 373 EPP, part. 29 IMCO) so as to ensure that any such negative consequences for affected parties do not go beyond what is strictly necessary to effectively address the significant risk identified. This should concern, in particular, a limitation to individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication in respect of whom there are reasonable grounds of suspicion for a link, even an indirect one, with child sexual abuse material as defined in Article 2 an identifiable part or component of the service where possible without prejudice to the effectiveness of the measure, such as specific types of channels of a publicly available number-independent (AM 374 ECR, part. 29 IMCO) interpersonal communications service, or to specific users or specific groups of users, to the extent that they can be taken in isolation for the purpose of detection, as well as the specification of the safeguards additional to the ones already expressly specified in this Regulation, such as independent auditing, the provision of additional information or access to data, or reinforced human oversight and review, and the further limitation of the duration of application of the detection order that the Coordinating Authority deems necessary. To avoid unreasonable or disproportionate outcomes, such requirements should be set after an objective and diligent assessment conducted on a case-by-case basis.

Recitals 24
Covers: partially 376 (Greens), partially 32 (IMCO)
Falls: AMs 375 (The Left)
regarding the technologies that a provider envisages deploying and operating to execute a detection order addressed to it under this Regulation.

Recital 25

Covers: 377 (Greens), 378 (The Left), 33 (IMCO)

Falls: none

(25) Where new services are concerned, that is, services not previously offered in the Union, the evidence available on the potential misuse of the service in the last 12 months is normally non-existent. Taking this into account, and to ensure the effectiveness of this Regulation, the Coordinating Authority should be able to draw on evidence stemming from comparable services when assessing whether to request the issuance of a detection order in respect of such a new service. A service should be considered comparable where it provides a functional equivalent to the service in question, having regard to all relevant facts and circumstances, in particular its main characteristics and functionalities, the manner in which it is offered and used, the user base, the applicable terms and conditions and risk mitigation measures, as well as the overall remaining risk profile. (AMs 377 Greens, 378 The Left, 33 IMCO)