



2022/0155(COD)

28.7.2023

AMENDMENTS

277 - 544

Draft report
Javier Zarzalejos
(PE746.811v01-00)

Laying down rules to prevent and combat child sexual abuse

Proposal for a regulation
(COM(2022)0209 – C9-0174/2022 – 2022/0155(COD))

Amendment 277

Rob Rooken

Proposal for a regulation

—

Proposal for rejection

***The European Parliament rejects the
Commission proposal (COM(2022)0209).***

Or. en

Justification

Withdraw this proposal for a Regulation and replace it with a proposal to tackle child sexual abuse online which has an appropriate legal basis, which is technically feasible, and which is not manifestly incompatible with the EU prohibition of general monitoring obligations.

Amendment 278

Clare Daly, Cornelia Ernst

Proposal for a regulation

—

Proposal for rejection

***The European Parliament rejects the
Commission proposal (COM(2022)0209).***

Or. en

Justification

Calls on the Commission to replace it with a proposal to tackle child sexual abuse online which has an appropriate legal basis; which is built on sustained engagement with child rights' specialists and in particular specialists on children's digital rights, human rights and digital rights groups more broadly, experts in cybersecurity and technology, and experts in internet regulation; which is technically feasible; and which is not manifestly incompatible with the Charter of Fundamental Rights and the EU prohibition of general monitoring obligations.

Amendment 279

Charlie Weimers, Cristian Terheş, Rob Rooken

Proposal for a regulation

–

Proposal for rejection

The European Parliament rejects the Commission proposal (COM(2022)0209).

Or. en

Amendment 280

Moritz Körner, Sophia in 't Veld, Yana Toom, Morten Petersen, Michal Šimečka, Jan-Christoph Oetjen, Svenja Hahn, Karen Melchior

Proposal for a regulation

–

Proposal for rejection

The European Parliament rejects the Commission proposal (COM(2022)0209).

Or. en

Justification

The complementary impact assessment of the proposal, requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs finds: (1) Weaknesses in the argumentation (problem definition) underpinning the CSA proposal; (2) The fact that the proposal targets known content, new content, and grooming, while the technologies to detect new content and grooming are of low accuracy (compared to the technologies to detect known CSAM). A majority of experts consulted consider that deploying the technologies to detect new CSAM and grooming will result in an increase in reported content and a reduction in accuracy, thereby substantially impacting law enforcement agencies' (LEAs) workload. The feasibility of the role of an EU centre in filtering reported content specifically to alleviate the burden on LEAs is questioned; (3) The fact that perpetrators that are keen to continue their activities and will likely resort to the dark and deep web where identification is more complicated to avoid being targeted by the measures introduced by the CSA proposal. (4) The detection of CSAM in end-to-end encryption (E2EE) raises fundamental issues with regards to the secure nature of E2EE, as it creates vulnerabilities for users of E2EE communication channels; (5) Weighing all the fundamental rights affected by the inclusion of the measures in the CSA proposal, it can be concluded that the CSA proposal would interfere with Articles 7 and 8 of the Charter of Fundamental Rights of the EU. This interference, by violating the prohibition on general data retention and the prohibition against general monitoring obligations, cannot be justified.

Amendment 281

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Title 1

Text proposed by the Commission

Proposal for a
REGULATION OF THE EUROPEAN
PARLIAMENT AND OF THE COUNCIL
laying down rules to **prevent and combat**
child sexual abuse
(Text with EEA relevance)

Amendment

Proposal for a
REGULATION OF THE EUROPEAN
PARLIAMENT AND OF THE COUNCIL
laying down rules to **address online** child
sexual abuse
(Text with EEA relevance)

Or. en

Justification

Aligned with title of Terrorist Content Online Regulation: „address“ is more realistic than claiming to be able to „prevent“ CSA; added „online“ to separate from the 2011 Directive that regulates criminal law and actual offline child sexual abuse.

Amendment 282

Sophia in 't Veld, Moritz Körner

Proposal for a regulation

Citation 1

Text proposed by the Commission

Having regard to the Treaty on the
Functioning of the European Union, and in
particular Article 114 thereof,

Amendment

Having regard to the Treaty on the
Functioning of the European Union, and in
particular Article **16 and Article** 114
thereof,

Or. en

Amendment 283

Annalisa Tardino

Proposal for a regulation

Recital 1

Text proposed by the Commission

(1) Information society services have become very important for communication, expression, gathering of information and many other aspects of present-day life, including for children but also for perpetrators of child sexual abuse offences. Such offences, which are subject to minimum rules set at Union level, are very serious criminal offences that need to be prevented and combated effectively in order to protect children's rights and well-being, as is required under the Charter of Fundamental Rights of the European Union ('Charter'), and to protect society at large. Users of such services offered in the Union should be able to trust that the services concerned can be used safely, especially by children.

Amendment

(1) Information society services have become very important for communication, expression, gathering of information and many other aspects of present-day life, including for children but also for perpetrators of child sexual abuse offences. Such offences, which are subject to minimum rules set at Union level, are very serious criminal offences that ***often cause long-lasting negative consequences on victims that*** need to be prevented and combated effectively in order to protect children's rights and well-being, as is required under the Charter of Fundamental Rights of the European Union ('Charter'), ***and also in order to avoid the risk of secondary victimisation*** and to protect society at large. Users of such services offered in the Union should be able to trust that the services concerned can be used safely, especially by children.

Or. en

Amendment 284
Maria Grapini

Proposal for a regulation
Recital 1

Text proposed by the Commission

(1) Information society services have become very important for communication, expression, gathering of information and many other aspects of present-day life, including for children but also for perpetrators of child sexual abuse offences. Such offences, which are subject to minimum rules set at Union level, are very serious criminal offences that need to be prevented and combated effectively in order to protect children's rights and well-being, as is required under the Charter of Fundamental Rights of the European Union

Amendment

(1) Information society services have become very important for communication, expression, gathering of information and many other aspects of present-day life, including for children but also for perpetrators of child sexual abuse offences. Such offences, which are subject to minimum rules set at Union level, are very serious criminal offences that need to be prevented and combated effectively in order to protect children's rights and well-being, as is required under the Charter of Fundamental Rights of the European Union

(‘Charter’), and to protect society at large. Users of such services offered in the Union should be able to trust that the services concerned can be used safely, especially by children.

(‘Charter’), and to protect society at large. Users of such services offered in the Union ***must have the assurance that they are protected against any type of sexual abuse in the online environment, and*** should be able to trust that the services concerned can be used safely, especially by children.

Or. ro

Amendment 285

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Recital 1 a (new)

Text proposed by the Commission

Amendment

(1a) When using artificial intelligence algorithms on images, it is well documented that bias and discrimination can occur due to the lack of representativeness of certain population groups in the data used to train the algorithm. These biases should be identified, measured and eradicated in order for the detection systems to be truly profitable to society as a whole.

Or. en

Amendment 286

Annika Bruna

Proposal for a regulation

Recital 1 a (new)

Text proposed by the Commission

Amendment

(1a) It should be specified that over 60 % of the images of child sexual abuse

circulating in the world are hosted in the EU, and that 1 out of 5 children in Europe are victims of sexual violence and abuse, reflecting the urgent need for rules to be laid down in the EU.

Or. fr

Amendment 287

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Recital 1 b (new)

Text proposed by the Commission

Amendment

(1b) The use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of relevant information society services or on any other organisations with regard to any level of the supply chain that would result in the weakening of the security of their networks and services, such as bypassing authentication and accessing encrypted data or creating deliberate weaknesses by providers to allow for access to encrypted data.

Or. en

Amendment 288

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation
Recital 1 c (new)

Text proposed by the Commission

Amendment

(1c) End-to-end encryption is an important tool to guarantee the security and confidentiality of communications of users, including those of children. Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption.

Or. en

Amendment 289
Vincenzo Sofo, Charlie Weimers, Jadwiga Wiśniewska

Proposal for a regulation
Recital 2

Text proposed by the Commission

Amendment

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent and combat such abuse. The measures taken should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent and combat such abuse. The measures taken should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services. ***Considering the***

importance of the right to privacy, including the protection of personal data, as guaranteed by the Charter of Fundamental Rights, nothing in this regulation should be interpreted in a way that would enable future broad based mass surveillance.

Or. en

Amendment 290

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 2

Text proposed by the Commission

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being *the only ones* in a position to prevent and combat such abuse. The measures taken should be targeted, carefully balanced *and* proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

Amendment

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being in a position to prevent and *to help* combat such abuse. The measures taken should be targeted, carefully balanced, *effective, evidence-based, proportionate, and subject to constant review*, so as to avoid any undue negative consequences *for the fight against crime and* for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid *directly or indirectly* imposing any excessive burdens on the providers of the services.

Or. en

Justification

It is never the case that information society service providers are the only ones in a position to prevent or combat abuse. Relying exclusively on profit-motivated private companies for investigation and prosecution of serious crimes, rather than the forces of law and order, is dangerous.

Amendment 291

Maria Grapini

Proposal for a regulation

Recital 2

Text proposed by the Commission

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures *to* minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent and combat such abuse. The measures taken should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

Amendment

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures *that offer users greater security and* minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent and combat such abuse. The measures taken should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

Or. ro

Amendment 292

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 2

Text proposed by the Commission

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual **abuse, those providers often being the only ones in a position to prevent and combat such** abuse. The measures taken should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

Amendment

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual abuse. The measures taken should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

Or. en

Amendment 293

Maria Grapini

Proposal for a regulation

Recital 2

Text proposed by the Commission

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent **and combat** such abuse. The measures taken should be targeted,

Amendment

(2) Given the central importance of relevant information society services, those aims can only be achieved by ensuring that providers offering such services in the Union behave responsibly and take reasonable, **reliable and tangible** measures to minimise the risk of their services being misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent, **combat and report** such abuse. The measures taken

carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

should be targeted, carefully balanced and proportionate, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

Or. ro

Amendment 294
Annika Bruna

Proposal for a regulation
Recital 2 a (new)

Text proposed by the Commission

Amendment

(2a) A long-term solution should be envisaged, within a proportionate legal framework in which automated technology should be used to detect, in a secure manner, online sexual exploitation and abuse.

Or. fr

Amendment 295
Maria Grapini

Proposal for a regulation
Recital 3

Text proposed by the Commission

Amendment

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In

the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level, ***offering internet users greater security in terms of combating online child sex abuse.***

Or. ro

Amendment 296
Annalisa Tardino

Proposal for a regulation
Recital 3

Text proposed by the Commission

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, have a ***direct*** negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the ***necessary*** harmonised requirements should be laid down at Union level.

Amendment

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse ***and more generally to safeguard minors online***, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which ***sometimes*** diverge, ***may*** have a negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the harmonised requirements should be laid down at Union level.

Or. en

Amendment 297

Carles Puigdemont i Casamajó

Proposal for a regulation

Recital 3

Text proposed by the Commission

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

Amendment

(3) Member States **and regional authorities** are increasingly introducing, or are considering introducing, national **and regional** laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, **may** have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

Or. en

Amendment 298

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 3

Text proposed by the Commission

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws,

Amendment

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws,

which diverge, have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

which diverge, *may* have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

Or. en

Amendment 299

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 3

Text proposed by the Commission

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

Amendment

(3) Member States are increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, *may* have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

Or. en

Amendment 300

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 4

Text proposed by the Commission

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. ***In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper innovation.***

Amendment

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned.

Or. en

Amendment 301
Annalisa Tardino

Proposal for a regulation
Recital 4

Text proposed by the Commission

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, ***so as not to hamper innovation.***

Amendment

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective, ***proportionate and coherent with national legislations*** and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, ***in order to stimulate the development of innovative instruments to tackle child sexual abuse.***

Or. en

Amendment 302

Proposal for a regulation

Recital 4

Text proposed by the Commission

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper innovation.

Amendment

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective, ***well targeted and proportionate*** and that respects the fundamental rights ***and privacy*** of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper innovation.

Or. en

Amendment 303

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 4

Text proposed by the Commission

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper ***innovation***.

Amendment

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is ***demonstrably and durably*** effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper ***the fight against crime***.

Amendment 304
Maria Grapini

Proposal for a regulation
Recital 4

Text proposed by the Commission

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent **and combat** child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper innovation.

Amendment

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent, **combat and report** child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper innovation.

Or. ro

Amendment 305
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission

Amendment

(4a) To ensure full achievement of the objectives of this Regulation, Member States should introduce and implement prevention strategies and awareness campaigns in their schools and educational institutions. The EU Centre and Coordinating Authorities, in close cooperation with relevant stakeholders, such as law enforcement agencies and existing hotlines across the Union, should elaborate prevention techniques, in order

to prevent and combat child sexual abuse. It is important that digital skills and competences, including media literacy, are recognised as a mandatory skill and an essential part of education, focusing on educating children, parents and educators and the general public on online safety, including online parental control and how to recognize and report online solicitation. The Union and its Member States should allocate more investment in education and training to ensure digital literacy, including protection from bullying and cyberbullying in schools, for children of different age groups.

Or. en

Amendment 306

Annika Bruna

Proposal for a regulation

Recital 4 a (new)

Text proposed by the Commission

Amendment

(4a) Protecting children online should not preclude respect for user privacy. The proposal should not impose a general control requirement but one of control in specific cases, based on the risk involved.

Or. fr

Amendment 307

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 5

Text proposed by the Commission

Amendment

(5) In order to achieve the objectives of this Regulation, it should cover providers

(5) In order to achieve the objectives of this Regulation, it should cover providers

of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services should include publicly available interpersonal communications services, *such as messaging services and web-based e-mail services, in so far as those service as publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.*

of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services should include publicly available ***number independent*** interpersonal communications services.

Or. en

Amendment 308

Sara Skyttedal, David Lega, Andrey Kovatchev, Tomáš Zdechovský, Stefan Berger, Christian Doleschal, Helmut Geuking, Ivan Štefanec, Peter Pollák, Johan Nissinen, Karen Melchior

Proposal for a regulation

Recital 5

Text proposed by the Commission

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services

Amendment

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services

should include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those services are publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.

should include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those services are publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. ***Online search engines and other artificial intelligence services should also be covered.*** However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate ***and targeted*** manner. ***Considering the fundamental importance of the right to respect for private life and the right to protection of personal data, as guaranteed by the Charter of Fundamental Rights, nothing in this regulation should be interpreted as prohibiting or compromising the integrity and confidentiality of end-to-end encrypted content and communications.***

Or. en

Justification

The integrity and confidentiality of end-to-end encrypted content and communications are essential for the confidentiality of digital correspondence and hence a prerequisite for the right to respect for private and family life and the right to protection of personal data as enshrined in Articles 7 and 8 of the Charter of the Fundamental Rights of the European Union (2000/C364/01). Client-side scanning with side-channel leaks is an example of a practice that, while not necessarily 'weakening' the end-to-end encryption, still puts the integrity and confidentiality of the end-to-end encrypted content and communications at risk.

Amendment 309
Annalisa Tardino

Proposal for a regulation
Recital 5

Text proposed by the Commission

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services should include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those service as publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.

Amendment

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services should include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those service as publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner ***without lowering child protection standards.***

Or. en

Amendment 310
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 5

Text proposed by the Commission

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that **have the potential to be** misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services **should** include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those **service as** publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are **equally** at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.

Amendment

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that **are** misused **to a significant extent** for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services **could** include publicly available **number-independent** interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those **services are** publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are **also** at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.

Or. en

Justification

It is illogical to refer to varying risks and equal risks when referring to the same range of services.

Amendment 311
Rob Rooken

Proposal for a regulation
Recital 5

Text proposed by the Commission

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services should include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those service as publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.

Amendment

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services should include publicly available **number independent** interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those service as publicly available. As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner.

Or. en

Amendment 312
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 6

Text proposed by the Commission

(6) Online child sexual abuse frequently involves the misuse of information society services offered in the Union by providers established in third

Amendment

(6) Online child sexual abuse frequently involves the misuse of information society services offered in the Union by providers established in third

countries. In order to ensure the effectiveness of the rules laid down in this Regulation ***and a level playing field within the internal market***, those rules should apply to all providers, irrespective of their place of establishment or residence, that offer services in the Union, as evidenced by a substantial connection to the Union.

countries. In order to ensure the effectiveness of the rules laid down in this Regulation, those rules should apply to all providers, irrespective of their place of establishment or residence, that offer services in the Union, as evidenced by a substantial connection to the Union.

Or. en

Amendment 313

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 6

Text proposed by the Commission

(6) Online child sexual abuse ***frequently involves*** the misuse of information society services offered in the Union by providers established in third countries. In order to ensure the effectiveness of the rules laid down in this Regulation and a level playing field within the internal market, those rules should apply to all providers, irrespective of their place of establishment or residence, that offer services in the Union, as evidenced by a substantial connection to the Union.

Amendment

(6) Online child sexual abuse ***can also involve*** the misuse of information society services offered in the Union by providers established in third countries. In order to ensure the effectiveness of the rules laid down in this Regulation and a level playing field within the internal market, those rules should apply to all providers, irrespective of their place of establishment or residence, that offer services in the Union, as evidenced by a substantial connection to the Union.

Or. en

Amendment 314

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 7

Text proposed by the Commission

(7) This Regulation should be without

Amendment

(7) This Regulation should be without

prejudice to the rules resulting from other Union acts, in particular Directive 2011/93 of the European Parliament and of the Council³⁸, Directive 2000/31/EC of the European Parliament and of the Council³⁹ and Regulation (EU) .../... of the European Parliament and of the Council⁴⁰ [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC], Directive 2010/13/EU of the European Parliament and of the Council⁴¹, Regulation (EU) 2016/679 of the European Parliament and of the Council⁴², and Directive 2002/58/EC of the European Parliament and of the Council⁴³.

prejudice to the rules resulting from other Union acts, in particular Directive 2011/93 of the European Parliament and of the Council³⁸, Directive 2000/31/EC of the European Parliament and of the Council³⁹ and Regulation (EU) **2022/2065** of the European Parliament and of the Council⁴⁰ [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC], Directive 2010/13/EU of the European Parliament and of the Council⁴¹, Regulation (EU) 2016/679 of the European Parliament and of the Council⁴², and Directive 2002/58/EC of the European Parliament and of the Council⁴³.

(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)

³⁸ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

³⁹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

⁴⁰ Regulation (EU) .../... of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (OJ L ...).

⁴¹ Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media service (OJ L 95, 15.4.2010, p. 1).

³⁸ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

³⁹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

⁴⁰ Regulation (EU) **2022/2065** of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (OJ L ...).

⁴¹ Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media service (OJ L 95, 15.4.2010, p. 1).

⁴² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

⁴³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications') (OJ L 201, 31.7.2002, p. 37).

⁴² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

⁴³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications') (OJ L 201, 31.7.2002, p. 37).

Or. en

Amendment 315
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 9

Text proposed by the Commission

(9) Article 15(1) of Directive 2002/58/EC allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in certain specific provisions of that Directive relating to the confidentiality of communications when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, inter alia, to prevent, investigate, detect and prosecute criminal offences, provided certain conditions are met, including compliance with the Charter. Applying the requirements of that provision by analogy, this Regulation should limit the exercise of the rights and obligations provided for in Articles 5(1), (3) and 6(1) of Directive 2002/58/EC, insofar as strictly necessary to execute detection orders issued in

Amendment

deleted

accordance with this Regulation with a view to prevent and combat online child sexual abuse.

Or. en

Amendment 316

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 9

Text proposed by the Commission

(9) Article 15(1) of Directive 2002/58/EC allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in certain specific provisions of that Directive relating to the confidentiality of communications when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, inter alia, to prevent, investigate, detect and prosecute criminal offences, provided certain conditions are met, including compliance with the Charter. Applying the requirements of that provision by analogy, this Regulation should limit the exercise of the rights and obligations provided for in Articles 5(1), (3) and 6(1) of Directive 2002/58/EC, insofar as strictly necessary to execute detection orders issued in accordance with this Regulation with a view to prevent and combat online child sexual abuse.

Amendment

(9) Article 15(1) of Directive 2002/58/EC allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in certain specific provisions of that Directive relating to the confidentiality of communications when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, inter alia, to prevent, investigate, detect and prosecute criminal offences, provided certain conditions are met, including compliance with the Charter, ***which, inter alia, requires the specific measures to be provided for by law and genuinely achieve objectives of general interest.*** Applying the requirements of that provision by analogy, this Regulation should limit the exercise of the rights and obligations provided for in Articles 5(1), (3) and 6(1) of Directive 2002/58/EC, insofar as strictly necessary ***in line with Article 52 of the Charter,*** to execute detection orders issued in accordance with this Regulation with a view to prevent and combat online child sexual abuse.

Or. en

Amendment 317

Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 9 a (new)

Text proposed by the Commission

Amendment

(9a) Encryption, and especially end-to-end encryption, is an increasingly important tool to guarantee the security and confidentiality of the communications of all users, including children. Any restrictions or undermining of any kind of encryption, de jure or de facto, can be used and abused by malicious third parties. Nothing in this Regulation should be interpreted as prohibiting providers of information society services from using any kind of encryption on any part of their services, restricting or, undermining or bypassing such encryption in the sense of being detrimental to users' expectations of confidential and secure communication services. Providers of information society services should under no circumstances be prevented from providing their services using the highest standards of encryption, considering that such encryption is essential for trust in and security of the digital services.

Or. en

Amendment 318

Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 11

Text proposed by the Commission

Amendment

(11) A substantial connection to the Union should be considered to exist where the relevant information society services has an establishment in the Union or, in its absence, on the basis of the existence of a significant number of users in one or more

(11) A substantial connection to the Union should be considered to exist where the relevant information society services has an establishment in the Union or, in its absence, on the basis of the existence of a significant number of users in one or more

Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. *The targeting of activities towards a Member State could also be derived from the availability of a software application in the relevant national software application store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State.* A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1), point (c), of Regulation (EU) 1215/2012 of the European Parliament and of the Council⁴⁴. Mere technical accessibility of a website from the Union should not, alone, be considered as establishing a substantial connection to the Union.

⁴⁴ Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1), point (c), of Regulation (EU) 1215/2012 of the European Parliament and of the Council⁴⁴. Mere technical accessibility of a website from the Union should not, alone, be considered as establishing a substantial connection to the Union.

⁴⁴ Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

Or. en

Amendment 319

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 11

(11) A substantial connection to the Union should be considered to exist where the relevant information society services has an establishment in the Union or, in its absence, on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. The targeting of activities towards a Member State could also be derived from the availability of a software application in the relevant national software application store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1), point (c), of Regulation (EU) 1215/2012 of the European Parliament and of the Council⁴⁴. Mere technical accessibility of a website from the Union **should not**, alone, be considered as establishing a substantial connection to the Union.

(11) A substantial connection to the Union should be considered to exist where the relevant information society services has an establishment in the Union or, in its absence, on the basis of the existence of a significant number, **in relation to population size**, of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. The targeting of activities towards a Member State could also be derived from the availability of a software application in the relevant national software application store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1), point (c), of Regulation (EU) 1215/2012 of the European Parliament and of the Council⁴⁴. Mere technical accessibility of a website from the Union **cannot**, alone, be considered as establishing a substantial connection to the Union.

⁴⁴ Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

⁴⁴ Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

*Justification**More coherent alignment with the DSA***Amendment 320****Cornelia Ernst, Clare Daly****Proposal for a regulation****Recital 12***Text proposed by the Commission*

(12) For reasons of consistency and technological neutrality, the term ‘child sexual abuse material’ should for the purpose of this Regulation be defined as referring to any *type of material constituting child pornography or pornographic performance* within the meaning of Directive 2011/93/EU, which is capable of being disseminated through the use of hosting or interpersonal communication services. At present, such material typically consists of images or videos, *without it however being excluded that it takes other forms, especially in view of future technological developments.*

Amendment

(12) For reasons of consistency and technological neutrality, the term ‘child sexual abuse material’ should for the purpose of this Regulation be defined as referring to any *material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of a child for primarily sexual purposes or any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes; or a live exhibition aimed at an audience, including by means of information and communication technology, of a child engaged in real or simulated sexually explicit conduct; or the sexual organs of a child for primarily sexual purposes* within the meaning of Directive 2011/93/EU, which is capable of being disseminated through the use of hosting or interpersonal communication services. At present, such material typically consists of images or videos.

Amendment 321
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 13

Text proposed by the Commission

(13) The term ‘online child sexual abuse’ should cover *not* only the dissemination of material previously detected and confirmed as constituting child sexual abuse material (‘known’ material), *but also of material not previously detected that is likely to constitute child sexual abuse material but that has not yet been confirmed as such (‘new’ material), as well as activities constituting the solicitation of children (‘grooming’). That is needed in order to address not only past abuse, the re-victimisation and violation of the victims’ rights it entails, such as those to privacy and protection of personal data, but to also address recent, ongoing and imminent abuse, so as to prevent it as much as possible, to effectively protect children and to increase the likelihood of rescuing victims and stopping perpetrators.*

Amendment

(13) The term ‘online child sexual abuse’ should cover only the dissemination of material previously detected and confirmed as constituting child sexual abuse material (‘known’ material).

Or. en

Amendment 322
Annalisa Tardino

Proposal for a regulation
Recital 13

Text proposed by the Commission

(13) The term ‘online child sexual abuse’ should cover not only the dissemination of material previously detected and confirmed as constituting

Amendment

(13) The term ‘online child sexual abuse’ should cover not only the dissemination of material previously detected and confirmed as constituting

child sexual abuse material ('known' material), but also of material not previously detected that is likely to constitute child sexual abuse material but that has not yet been confirmed as such ('new' material), as well as activities constituting the solicitation of children ('grooming'). That is needed in order to address not only past abuse, the re-victimisation and violation of the victims' rights it entails, such as those to privacy and protection of personal data, but to also address recent, ongoing and imminent abuse, so as to prevent it as much as possible, to effectively protect children and to increase the likelihood of rescuing victims *and* stopping perpetrators.

child sexual abuse material ('known' material), but also of material not previously detected that is likely to constitute child sexual abuse material but that has not yet been confirmed as such ('new' material), as well as activities constituting the solicitation of children ('grooming'). That is needed in order to address not only past abuse, the re-victimisation and violation of the victims' rights it entails, such as those to privacy and protection of personal data, but to also address recent, ongoing and imminent abuse, so as to prevent it as much as possible, to effectively protect children and to increase the likelihood of rescuing victims, stopping *and prosecuting* perpetrators.

Or. en

Amendment 323
Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Recital 13 a (new)

Text proposed by the Commission

Amendment

(13a) In order to protect children, this Regulation should take into account the concerning hypersexualized use of children's images in advertising campaigns and the increasing spread of cultural pseudo-pedophilia also fuelled by fundraising campaigns.

Or. en

Amendment 324
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 14

Text proposed by the Commission

(14) With a view to minimising the risk that their services are misused for the dissemination of known or new child sexual abuse material or the solicitation of children, providers of hosting services and providers of publicly available interpersonal communications services should assess **such** risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements to be taken into account should be provided. **To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant.** As risks evolve over time, in function of developments such as those related to technology and the **manners** in which the services in question are offered and used, it is appropriate to ensure that the risk assessment **is** updated regularly and when needed for particular reasons.

Amendment

(14) With a view to minimising the risk that their services are misused for the dissemination of known or new child sexual abuse material or the solicitation of children, providers of hosting services and providers of publicly available **number-independent** interpersonal communications services should assess **the existence of a recurring systemic** risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements to be taken into account should be provided. As risks evolve over time, in function of developments such as those related to technology and the **manner** in which the services in question are offered and used, it is appropriate to ensure that the risk assessment, **as well as the effectiveness and proportionality of mitigation measures, are** updated regularly and when needed for particular reasons.

Or. en

Amendment 325
Annalisa Tardino

Proposal for a regulation
Recital 14

Text proposed by the Commission

(14) With a view to minimising the risk that their services are misused for the dissemination of known or new child sexual abuse material or the solicitation of children, providers of hosting services and providers of publicly available interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-

Amendment

(14) With a view to minimising the risk that their services are misused for the dissemination of known or new child sexual abuse material or the solicitation of children, providers of hosting services and providers of publicly available interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-

exhaustive list of elements to be taken into account should be provided. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment is updated regularly and when needed for particular reasons.

exhaustive list of elements to be taken into account should be provided ***based on best practices already enforced by Member States***. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment is updated regularly and when needed for particular reasons.

Or. en

Amendment 326
Rob Rooken

Proposal for a regulation
Recital 14

Text proposed by the Commission

(14) With a view to minimising the risk that their services are misused for the dissemination of known or new child sexual abuse material or the solicitation of children, providers of hosting services and providers of publicly available interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements to be taken into account should be provided. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment is updated regularly and

Amendment

(14) With a view to minimising the risk that their services are misused for the dissemination of known or new child sexual abuse material or the solicitation of children, providers of hosting services and providers of publicly available ***number independent*** interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements to be taken into account should be provided. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment is updated regularly and

when needed for particular reasons.

when needed for particular reasons.

Or. en

Amendment 327

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 14

Text proposed by the Commission

(14) With a view to minimising the risk that their services are misused for the dissemination of known *or new* child sexual abuse material *or the solicitation of children*, providers of hosting services and providers of publicly available interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements to be taken into account should be provided. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment is updated regularly and when needed for particular reasons.

Amendment

(14) With a view to minimising the risk that their services are misused for the dissemination of known child sexual abuse material, providers of hosting services and providers of publicly available *number independent* interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements to be taken into account should be provided. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment is updated regularly and when needed for particular reasons.

Or. en

Amendment 328

Hilde Vautmans, Fabienne Keller, Olivier Chastel, Lucia Ďuriš Nicholsonová, Nathalie Loiseau

Proposal for a regulation

Recital 14 a (new)

(14a) Given the severity of these crimes and the long-lasting negative consequences on the victims and the risk of revictimization as a result of the dissemination of known material, new material, as well as activities constituting the solicitation of children, it is essential that this Regulation provides specific obligations for providers of hosting service and providers of interpersonal communication services to prevent, detect, report and remove child sexual abuse material in all their services, including interpersonal communications services, which may also be covered by end-to-end encryption, in light of the prevalence of dissemination of child sexual abuse material, including the solicitation of children, in interpersonal communication services.

Or. en

Amendment 329

Javier Moreno Sánchez, Juan Fernando López Aguilar, Domènec Ruiz Devesa, Pietro Bartolo, Hilde Vautmans, Antonio López-Istúriz White, Milan Brglez, Helène Fritzon, Estrella Durá Ferrandis, Carina Ohlsson, Caterina Chinnici, Cyrus Engerer

**Proposal for a regulation
Recital 14 a (new)**

(14a) Given the severity of these crimes and the long-lasting negative consequences on the victims and the risk of revictimization as a result of the dissemination of known material, new material, as well as activities constituting the solicitation of children, it is essential that this Regulation provides specific obligations for providers of hosting services and providers of interpersonal communication services to prevent, detect, report, remove child sexual abuse

material in all their services, including interpersonal communication services, which may also be covered by end-to-end encryption, in light of the prevalence of dissemination of child sexual abuse material, including the solicitation of children, in interpersonal communication services.

Or. en

Amendment 330

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 15

Text proposed by the Commission

(15) Some of those providers of relevant information society services in scope of this Regulation may also be subject to an obligation to conduct a risk assessment under Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] with respect to information that they store and disseminate to the public. For the *purposes of the present Regulation, those providers may draw on such a risk assessment and complement it with a more specific assessment of the risks of use of their services for the purpose of online child sexual abuse, as required by this Regulation.*

Amendment

(15) Some of those providers of relevant information society services in scope of this Regulation may also be subject to an obligation to conduct a risk assessment under Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] with respect to information that they store and disseminate to the public, *which should form the basis* for the risk assessment *under this instrument.*

Or. en

Amendment 331

Annalisa Tardino

Proposal for a regulation

Recital 15

Text proposed by the Commission

(15) Some of those providers of relevant information society services in scope of this Regulation may also be subject to an obligation to conduct a risk assessment under Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] with respect to information that they store and disseminate to the public. For the purposes of the present Regulation, those providers may draw on such a risk assessment and complement it with a more specific assessment of the risks of use of their services for the purpose of online child sexual abuse, as required by this Regulation.

Amendment

(15) Some of those providers of relevant information society services in scope of this Regulation may also be subject to an obligation to conduct a risk assessment under Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] with respect to information that they store and disseminate to the public. For the purposes of the present Regulation ***and in order to avoid unnecessary burdens and duplications especially for SMEs***, those providers may draw on such a risk assessment and complement it with a more specific assessment of the risks of use of their services for the purpose of online child sexual abuse, as required by this Regulation.

Or. en

Amendment 332

Carles Puigdemont i Casamajó

Proposal for a regulation

Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... ***[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*** may consider to which extent mitigation measures adopted

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) **2022/2065** may consider to which extent mitigation measures adopted to comply with that obligation. ***Mitigation measures*** may include ***designing their online interfaces***

to comply with that obligation, *which* may include targeted measures to protect the rights of the child, including *age verification and* parental control tools, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

or parts thereof with the highest level of privacy, safety and security for children by default or adopting standards for protection of children, or participating in codes of conduct for protecting children, targeted measures to protect the rights of the child, including *functionalities enabling age assurance and age scoring, and age-appropriate* parental control tools. *Enabling flagging and/or notifying mechanisms and self-reporting functionalities* may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation. *Communication service providers (CSPs) may take voluntary measures to detect and remove child sexual abuse material (CSAM) from their services, provided that such measures are proportionate, necessary, and respectful of users' privacy and other fundamental rights. CSPs that take such measures shall comply with the following requirements:*(a) *Any measures taken to detect or remove CSAM must be based on clear, transparent, and publicly available criteria, which should be regularly reviewed and updated as necessary to reflect changes in technology and legal developments.*(b) *CSPs shall inform their users about the nature and extent of the measures taken to detect and remove CSAM, including any impact on users' privacy and other rights.*(c) *CSPs shall ensure that any measures taken to detect and remove CSAM are subject to appropriate oversight and accountability mechanisms, which should be designed to ensure that the measures are effective, proportionate, and respectful of users' rights.* (d) *CSPs shall cooperate with relevant competent authorities, including law enforcement authorities, to prevent and combat CSAM, and to support the identification and rescue of victims of child sexual exploitation and abuse.*

Amendment 333

Sara Skyttedal, David Lega, Andrey Kovatchev, Tomáš Zdechovský, Stefan Berger, Christian Doleschal, Helmut Geuking, Ivan Štefanec, Peter Pollák, Johan Nissinen, Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation**Recital 16***Text proposed by the Commission*

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... **[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]** may consider to which extent mitigation measures adopted to comply with that obligation, **which** may include targeted measures to protect the rights of the child, including **age verification and** parental control tools, **may also** serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take **effective and** reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) **2022/2065** may consider to which extent mitigation measures adopted to comply with that obligation. **Mitigation measures necessary for the fulfilment of the obligations in this regulation** may include **the design of online interfaces or parts thereof with the highest level of privacy, safety and security for children by default, the adaptation of standards for protection of children, participation in codes of conduct for protecting children,** targeted measures to protect the rights of the child, including **age-appropriate** parental control tools. **Enabling flagging and/or notifying mechanisms and self-reporting functionalities, where possible with the use of AI, shall** serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Justification

The measures taken by providers to mitigate the risk of their services being misused for abuse must, in addition to being reasonable, be effective in order to limit the encroachment on fundamental rights such as the right to privacy. Parental control remains an essential tool to mitigate the risk of abuse, and AI plays an increasingly important role for e.g. self-reporting functionalities like the one introduced by Apple in iOS 15 and Mac OS12 (Communications Safety).

Amendment 334

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate ***the risk of their services being misused for such abuse, as identified through the risk assessment.*** Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] ***may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification and parental control tools, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.***

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available ***number-independent*** interpersonal communications services should take reasonable ***specific*** measures to mitigate their services being misused for such abuse. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] ***should*** address the risk identified in the specific risk assessment.

Or. en

Amendment 335
Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification *and* parental control tools, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification, parental control tools *and functionalities enabling self-reporting by children, their parents or legal guardians*, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Or. en

Amendment 336
Annalisa Tardino

Proposal for a regulation
Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively,

Amendment

(16) In order to prevent and combat online child sexual abuse effectively,

providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification and parental control tools, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification and parental control tools, ***child friendly self reporting mechanisms*** may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Or. en

Amendment 337

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive

2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, ***including age verification and parental control tools***, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Or. en

Amendment 338
Rob Rooken

Proposal for a regulation
Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification and parental control tools, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available ***number independent*** interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, including age verification and parental control tools, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with

this Regulation.

Or. en

Amendment 339

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 16

Text proposed by the Commission

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, ***including age verification and parental control tools***, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Amendment

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available ***number independent*** interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

Or. en

Amendment 340

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 16 a (new)

Text proposed by the Commission

Amendment

(16a) To further prevent online child sexual abuse effectively, an emphasis should be placed on public awareness raising, including through easily understandable campaigns and in education with a focus on empowerment of young people to use the internet safely and to address societal factors that enable child sexual abuse, including harmful gender norms and broader issues of societal inequality; In addition awareness raising should focus on hotlines where young people can report what has happened to them, as well as to improve access to institutional reporting by police and social services and other authorities.

Or. en

Amendment 341

Annika Bruna

Proposal for a regulation

Recital 16 a (new)

Text proposed by the Commission

Amendment

(16a) Risk prevention should include the possibility to use approved technology that detects sexual content while respecting fundamental rights safeguards, including in end-to-end encrypted environments.

Or. fr

Amendment 342

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 17

Text proposed by the Commission

Amendment

(17) *To allow for innovation and ensure proportionality and technological neutrality, no exhaustive list of the compulsory mitigation measures should be established. Instead, providers should be left a degree of flexibility to design and implement measures tailored to the risk identified and the characteristics of the services they provide and the manners in which those services are used. In particular, providers are free to design and implement, in accordance with Union law, measures based on their existing practices to detect online child sexual abuse in their services and indicate as part of the risk reporting their willingness and preparedness to eventually being issued a detection order under this Regulation, if deemed necessary by the competent national authority.*

(17) Providers should be left a degree of flexibility to design and implement measures tailored to the risk identified and the characteristics of the services they provide and the manners in which those services are used, *taking into account the autonomy and rights of children and adapt their design, features and functions of services accordingly.*

Or. en

Amendment 343

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 17

Text proposed by the Commission

(17) To allow for innovation and ensure proportionality and technological neutrality, no exhaustive list of the compulsory *mitigation* measures should be established. Instead, providers should be left a degree of flexibility to design and implement measures tailored to the *risk identified* and the characteristics of the services they provide and the manners in which those services are used. In particular, providers are free to design and implement, in accordance with Union law, measures based on their existing practices *to detect online child sexual abuse in their services and indicate as part of the risk*

Amendment

(17) To allow for innovation and ensure proportionality and technological neutrality, no exhaustive list of the compulsory *specific* measures should be established. Instead, providers should be left a degree of flexibility to design and implement measures tailored to the *risks, exposure* and the characteristics of the services they provide and the manners in which those services are used. In particular, providers are free to design and implement, in accordance with Union law, measures based on their existing practices. *Specific measures could include providing technical measures and tools*

reporting their willingness and preparedness to eventually being issued a detection order under this Regulation, if deemed necessary by the competent national authority.

that allow users to manage their own privacy visibility, reachability and safety, such as mechanisms for users to block or mute other users, mechanisms that ask for confirmation before displaying certain content, tools that prompt or warn users.

Or. en

Amendment 344

Lucia Ďuriš Nicholsonová, Fabienne Keller

Proposal for a regulation

Recital 17

Text proposed by the Commission

(17) To allow for innovation and ensure proportionality and technological neutrality, no exhaustive list of the compulsory mitigation measures should be established. Instead, providers should be left a degree of flexibility to design and implement measures tailored to the risk identified and the characteristics of the services they provide and the manners in which those services are used. In particular, providers are free to design and implement, in accordance with Union law, measures based on their existing practices to detect online child sexual abuse in their services and indicate as part of the risk reporting their willingness and preparedness to eventually being issued a detection order under this Regulation, if deemed necessary by the competent national authority.

Amendment

(17) To allow for innovation and ensure proportionality and technological neutrality, no exhaustive list of the compulsory mitigation measures should be established. Instead, providers should be left a degree of flexibility to design and implement measures tailored to the risk identified and the characteristics of the services they provide and the manners in which those services are used. In particular, providers are free to design and implement, in accordance with Union law, measures based on their existing practices to detect **and prevent** online child sexual abuse in their services and indicate as part of the risk reporting their willingness and preparedness to eventually being issued a detection order under this Regulation, if deemed necessary by the competent national authority.

Or. en

Amendment 345

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 17 a (new)

Text proposed by the Commission

Amendment

(17a) While age verification tools may be one possible method of mitigating risk, many currently-known age verification methods create a risk of systemic violations of privacy and data protection. This includes, inter alia, the mass profiling of the users, the biometric analysis of the user's face and/or voice, or the deployment of digital identification/certification system, none of which currently respects individuals' fundamental rights sufficiently to justify its large-scale or mandatory deployment. Implementation of any of these measures by the providers of communication services would necessarily add another layer of interference with the rights and freedoms of the users, or unduly restrict access to services to people who appear younger or older than their actual age or people who do not have the necessary identification documents. As such, methods to verify or assess the age of users should not be mandatory, if used, be approached with caution and allow for alternatives, to ensure the protection of rights to privacy and data protection of all internet users in line with the GDPR, and to ensure that it remains possible for law-abiding internet users to remain anonymous.

Or. en

Amendment 346

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 17 b (new)

Text proposed by the Commission

Amendment

(17b) Relying on providers for risk mitigation measures comes with inherent risks, as business models, technologies and crimes evolve continuously. As a result, clear targets, oversight, review and adaptation, led by national supervisory authorities are needed, to avoid measures becoming redundant, disproportionate, ineffective, counterproductive and outdated.

Or. en

Amendment 347

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 18

Text proposed by the Commission

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on ***mitigation*** measures. Therefore, providers of hosting services and providers of publicly available interpersonal communications services should, when designing and implementing the ***mitigation*** measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which ***mitigation*** measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate ***mitigation*** measures, providers should at least duly consider the possible measures listed in this Regulation, ***as well***

Amendment

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on ***specific*** measures. Therefore, providers of hosting services and providers of publicly available ***number-independent*** interpersonal communications services should, when designing and implementing the ***specific*** measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which ***specific*** measures should reasonably be taken in a given situation, account should also be taken of ***the ongoing effectiveness of the measures***, the financial and technological capabilities and the size of the provider concerned. When selecting appropriate ***specific*** measures, providers should at least duly

as, where appropriate, other measures such as those based on industry best practices, including as established through self-regulatory cooperation, and those contained in guidelines from the Commission. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

consider the possible measures listed in this Regulation, *quantifying the expected impact of the available* measures. *Objective data on ongoing effectiveness must be provided, in order for any measure to be recognised as best practice.*

Or. en

Amendment 348
Rob Rooken

Proposal for a regulation
Recital 18

Text proposed by the Commission

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on mitigation measures. Therefore, providers of hosting services and providers of publicly available interpersonal communications services should, when designing and implementing the mitigation measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which mitigation measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate mitigation measures, providers should at least duly consider the possible measures listed in this Regulation, as well as, where appropriate, other measures such

Amendment

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on mitigation measures. Therefore, providers of hosting services and providers of publicly available **number independent** interpersonal communications services should, when designing and implementing the mitigation measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which mitigation measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate mitigation measures, providers should at least duly consider the possible measures listed in this Regulation, as well as, where appropriate, other

as those based on industry best practices, including as established through self-regulatory cooperation, and those contained in guidelines from the Commission. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

measures such as those based on industry best practices, including as established through self-regulatory cooperation, and those contained in guidelines from the Commission. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

Or. en

Amendment 349

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 18

Text proposed by the Commission

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on mitigation measures. Therefore, providers of hosting services and providers of publicly available interpersonal communications services should, when designing and implementing the mitigation measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which mitigation measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate mitigation measures, providers should at least duly consider the possible measures listed in this Regulation, as well as, where appropriate, other measures such as those based on industry best practices,

Amendment

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on mitigation measures. Therefore, providers of hosting services and providers of publicly available **number independent** interpersonal communications services should, when designing and implementing the mitigation measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which mitigation measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate mitigation measures, providers should at least duly consider the possible measures listed in this Regulation, as well as, where appropriate, other measures such as those based on industry

including as established through self-regulatory cooperation, and those contained in guidelines from the **Commission**. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

best practices, including as established through self-regulatory cooperation, and those contained in guidelines from the **EU Centre**. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

Or. en

Amendment 350

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 19

Text proposed by the Commission

Amendment

(19) *In the light of their role as intermediaries facilitating access to software applications that may be misused for online child sexual abuse, providers of software application stores should be made subject to obligations to take certain reasonable measures to assess and mitigate that risk. The providers should make that assessment in a diligent manner, making efforts that are reasonable under the given circumstances, having regard inter alia to the nature and extent of that risk as well as their financial and technological capabilities and size, and cooperating with the providers of the services offered through the software application where possible.*

deleted

Or. en

Amendment 351

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 19

Text proposed by the Commission

Amendment

(19) In the light of their role as intermediaries facilitating access to software applications that may be misused for online child sexual abuse, providers of software application stores should be made subject to obligations to take certain reasonable measures to assess and mitigate that risk. The providers should make that assessment in a diligent manner, making efforts that are reasonable under the given circumstances, having regard inter alia to the nature and extent of that risk as well as their financial and technological capabilities and size, and cooperating with the providers of the services offered through the software application where possible.

deleted

Or. en

Amendment 352

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 20

Text proposed by the Commission

Amendment

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures 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 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

deleted

limits and safeguards. For instance, considering that child sexual abuse material tends to be disseminated through hosting services and publicly available interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

Or. en

Amendment 353

Sara Skyttedal, David Lega, Andrey Kovatchev, Tomáš Zdechovský, Stefan Berger, Christian Doleschal, Helmut Geuking, Ivan Štefanec, Peter Pollák, Johan Nissinen, Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari, Karen Melchior

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures **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 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 interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it should only be possible to address detection orders to

Amendment

(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** 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**, 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 interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it

providers of such services.

should only be possible to address detection orders to providers of such services. ***Such detection orders shall be issued with regards to the technical capacity of the provider, and shall in no way be interpreted as prohibiting, or compromising the integrity and confidentiality of, end-to-end encrypted content and communications.***

Or. en

Justification

As proposed by the rapporteur, the issuance of detection orders should be only a measure of last resort. Detection orders must be possible to comply with, taking into account the technical capacity of the service provider. In accordance with the proposed Article 6a, they must never be interpreted as prohibiting, or compromising the integrity and confidentiality of, end-to-end encrypted content and communications. Client-side scanning with side-channel leaks is an example of a practice that, while not necessarily 'weakening' the end-to-end encryption, still puts the integrity and confidentiality of the end-to-end encrypted content and communications at risk.

Amendment 354

Rob Rooken

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures 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 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***

Amendment

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures are deemed insufficient to limit the risk of misuse of a certain service for the purpose of online child sexual abuse, ***and where the provider refuses to cooperate with Coordinating Authorities and the Centre,*** the Coordinating Authorities designated by Member States under this Regulation should be empowered to request the issuance of detection orders ***as a last resort.*** 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

be disseminated through hosting services and publicly available interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

limits and safeguards.

Or. en

Justification

This recital specifies that the detection orders shall only be issued to providers that do not cooperate or fail to comply with their obligations,

and as a last resort. Detection orders are extremely intrusive for citizens.

Amendment 355

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) With a view to ensuring effective prevention and fight against ***online child sexual abuse, when mitigating measures 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 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 interpersonal communications services, ***and that solicitation of children mostly takes place***

Amendment

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, the Coordinating Authorities designated by Member States under this Regulation should be empowered to request the issuance of detection orders ***targeting suspects***. 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 ***targets***, limits and safeguards. For instance, considering that child sexual abuse material tends to be disseminated through hosting services and publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

in publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

Or. en

Amendment 356

Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures 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 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 interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

Amendment

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures 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 the issuance of detection orders. ***Such orders should not apply to end-to-end encryption services.*** 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 interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

Or. en

Amendment 357

Paul Tang, Alex Agius Saliba

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures 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 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 interpersonal communications services, and that solicitation of children mostly takes place in** publicly available interpersonal communications services, it should only be possible to address detection **orders** to providers of such services.

Amendment

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures 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 the issuance of detection **warrants**. 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 **number-independent** publicly available interpersonal communications services, it should only be possible to address detection **warrants** to providers of such services.

Or. en

Justification

This amendment should be interpreted as changing the wording "detection orders" throughout this Regulation to "detection warrants". Detection warrants target specific devices or specific user accounts of an individual suspect against which there is a reasonable suspicion of possessing "known child sexual abuse material". Those warrants can only be issued by competent judicial authorities.

Amendment 358

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Recital 20 a (new)

Text proposed by the Commission

Amendment

(20a) End-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be prohibiting or weakening end-to-end encryption or be interpreted in that way.

Or. en

Amendment 359
Paul Tang, Alex Agius Saliba

Proposal for a regulation
Recital 20 b (new)

Text proposed by the Commission

Amendment

(20b) The use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations, at any level of the supply chain, that would result in the weakening of the security of their networks and services, such as the creation or facilitation of backdoors or any other functionality allowing disclosure of communications content to third parties.

Or. en

Amendment 360
Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation
Recital 20 c (new)

Text proposed by the Commission

Amendment

(20c) The act of breaking encryption refers to the act of defeating or bypassing the encryption protocol used to secure a communication. Any access by any third-party that was not meant to access, read or edit the content of that communication that was supposed to be private and secure should be considered as undermining encryption.

Or. en

Amendment 361
Paul Tang, Alex Agius Saliba

Proposal for a regulation
Recital 20 d (new)

Text proposed by the Commission

Amendment

(20d) The technologies used for the purpose of executing detection warrants should be in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default pursuant to Regulation (EU) 2016/679.

Or. en

Amendment 362
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 21

Text proposed by the Commission

Amendment

(21) Furthermore, as parts of those

deleted

limits and safeguards, detection orders should only be issued after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for a given type of online child sexual abuse covered by this Regulation. 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 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.

Or. en

Amendment 363

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 21

Text proposed by the Commission

(21) Furthermore, as parts of those limits and safeguards, detection orders should *only be issued after a diligent and objective assessment leading to the finding of a significant risk* of the *specific service concerned* being *misused for a given type* of online child sexual abuse covered by this Regulation. *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*

Amendment

(21) Furthermore, as parts of those limits and safeguards, detection orders should *require a reasonable suspicion* of the service being *used for the purpose* of online child sexual abuse *by one or more suspects*.

types of online child sexual abuse at stake 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.

Or. en

Amendment 364

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Recital 21

Text proposed by the Commission

(21) Furthermore, as parts of those limits and safeguards, detection *orders* should only be issued *after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for a given type of online child sexual abuse covered by this Regulation*. 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 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.*

Amendment

(21) Furthermore, as parts of those limits and safeguards, detection *warrants* should only be issued *by a judicial authority and only with the purpose to detect known online child sexual abuse material related to a specific device or user account, where there is a reasonable suspicion such content is stored on that device or in that user account*. One of the *main* elements to be taken into account in this regard is the *existence of evidence demonstrating a reasonable suspicion that individual accounts or groups of accounts are being used for the purpose of online child sexual abuse*.

Or. en

Justification

This amendment should be interpreted as changing the wording "detection orders" throughout this Regulation to "detection warrants". Detection warrants target specific devices or specific user accounts of an individual suspect against which there is a reasonable suspicion of possessing "known child sexual abuse material". Those warrants can only be

issued by competent judicial authorities.

Amendment 365

Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation

Recital 21

Text proposed by the Commission

(21) Furthermore, as parts of those limits and safeguards, detection orders should only be issued after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for a given type of online child sexual abuse covered by this Regulation. 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 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.

Amendment

(21) Furthermore, as parts of those limits and safeguards, detection orders should only be issued after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for a given type of online child sexual abuse covered by this Regulation. ***Such detection orders should as far as possible be restricted and specified, not calling for mass detection.*** 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 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.

Or. en

Amendment 366

Annalisa Tardino

Proposal for a regulation

Recital 21

Text proposed by the Commission

(21) Furthermore, as parts of those

Amendment

(21) Furthermore, as parts of those

limits and safeguards, detection orders should only be issued after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for a given type of online child sexual abuse covered by this Regulation. 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 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.

limits and safeguards, detection orders should only be issued after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for a given type of online child sexual abuse covered by this Regulation. 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*** 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.

Or. en

Amendment 367

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 22

Text proposed by the Commission

(22) However, the finding of such 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 authority or independent administrative authority having objectively and diligently

Amendment

deleted

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 at issue, but also the likelihood and seriousness of any potential negative consequences for other parties affected. 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.

Or. en

Amendment 368

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Recital 22

Text proposed by the Commission

(22) However, the ***finding of such 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 ***authority or independent administrative authority*** 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 at issue, but also the ***likelihood and seriousness of any potential negative consequences for other parties affected***. With a view to avoiding the imposition of

Amendment

(22) However, the ***existence of evidence demonstrating a reasonable suspicion that individual accounts or groups of accounts are being used for the purpose of online child sexual abuse*** should in itself be insufficient to justify the issuance of a detection ***warrant***, 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 ***warrants*** can be issued only after the Coordinating Authorities and the competent judicial authority 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 at issue, but also the ***actual or potential implications for the rights and legitimate***

excessive burdens, the assessment should also take account of the financial and technological capabilities and size of the provider concerned.

interests of all parties concerned, including the possible failure of the measures to respect the fundamental rights enshrined in the Charter. 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.

Or. en

Justification

This amendment should be interpreted as changing the wording "detection orders" throughout this Regulation to "detection warrants". Detection warrants target specific devices or specific user accounts of an individual suspect against which there is a reasonable suspicion of possessing "known child sexual abuse material". Those warrants can only be issued by competent judicial authorities.

Amendment 369

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 22

Text proposed by the Commission

(22) However, the finding of such 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 **authority or independent administrative** authority 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

Amendment

(22) However, the finding of such **evidence** should in itself be insufficient to justify the issuance of a detection order. Therefore, it should be ensured that detection orders can be issued only after the Coordinating Authorities and the competent judicial authority 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 at issue, but also **the specific results anticipated by the measure,** the likelihood and seriousness of any potential negative consequences for other parties affected. With a view to avoiding the imposition of excessive

for the type of online child sexual abuse at issue, but also the likelihood and seriousness of any potential negative consequences for other parties affected. 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.

burdens, the assessment should also take account of the financial and technological capabilities and size of the provider concerned.

Or. en

Amendment 370

Maite Pagazaurtundúa, Moritz Körner

Proposal for a regulation

Recital 22

Text proposed by the Commission

(22) However, the finding of such 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 **authority or independent administrative** authority 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 at issue, but also the likelihood and seriousness of any potential negative consequences for other parties affected. 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

Amendment

(22) However, the finding of such 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 authority 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 at issue, but also the likelihood and seriousness of any potential negative consequences for other parties affected. 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.

provider concerned.

Or. en

Amendment 371
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 23

Text proposed by the Commission

Amendment

(23) 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 targeted and specified 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 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 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

deleted

basis.

Or. en

Amendment 372

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 23

Text proposed by the Commission

(23) 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 targeted ***and*** specified 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 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 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

Amendment

(23) 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 targeted, ***has quantifiable targets, is limited in time and is*** specified so as to ensure that any such negative consequences for affected parties do not go beyond what is strictly necessary to effectively ***and demonstrably mitigate*** the significant risk identified. This should concern, in particular, a limitation to an identifiable ***user or users***. Safeguards additional to the ones already expressly specified in this Regulation ***should in addition be specified***. Independent auditing, ***in particular of the achievement of the anticipated results***, the provision of additional information or access to data, reinforced human oversight and review, and the further limitation of the duration of application of the detection order ***should be prerequisites of such orders being made***. To avoid unreasonable or disproportionate outcomes, such requirements should be set after an objective and diligent assessment conducted on a case-by-case basis.

conducted on a case-by-case basis.

Or. en

Amendment 373

Sara Skyttedal, David Lega, Andrey Kovatchev, Tomáš Zdechovský, Stefan Berger, Christian Doleschal, Helmut Geuking, Ivan Štefanec, Peter Pollák, Johan Nissinen, Karen Melchior, Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation

Recital 23

Text proposed by the Commission

(23) 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 targeted and *specified* 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 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 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

Amendment

(23) 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 *justified, proportionate and related only to an identifiable part of the specific service, user or group of users, as well as* targeted and *limited in time* 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 an identifiable part or component of the service, such as specific types of channels of a publicly available 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

conducted on a case-by-case basis.

after an objective and diligent assessment
conducted on a case-by-case basis.

Or. en

Justification

Detection orders must be justified, proportionate, targeted and limited in time, as well as related to an identifiable part of the specific service, user or group of users, in order to limit the encroachment on fundamental rights such as the right to privacy.

Amendment 374 **Rob Rooken**

Proposal for a regulation **Recital 23**

Text proposed by the Commission

(23) 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 targeted and specified 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 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 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

Amendment

(23) 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 targeted and specified 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 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*** 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,

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.

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.

Or. en

Amendment 375
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 24

Text proposed by the Commission

Amendment

(24) The competent judicial authority or the competent independent administrative authority, as applicable in accordance with the detailed procedural rules set by the relevant Member State, should be in a position to take a well-informed decision on requests for the issuance of detections orders. That is of particular importance to ensure the necessary fair balance of the fundamental rights at stake and a consistent approach, especially in connection to detection orders concerning the solicitation of children. Therefore, a procedure should be provided for that allows the providers concerned, the EU Centre on Child Sexual Abuse established by this Regulation ('EU Centre') and, where so provided in this Regulation, the competent data protection authority designated under Regulation (EU) 2016/679 to provide their views on the measures in question. They should do so as soon as possible, having regard to the important public policy objective at stake and the need to act without undue delay to protect children. In particular, data protections authorities should do their utmost to avoid extending the time period set out in

deleted

Regulation (EU) 2016/679 for providing their opinions in response to a prior consultation. Furthermore, they should normally be able to provide their opinion well within that time period in situations where the European Data Protection Board has already issued guidelines regarding the technologies that a provider envisages deploying and operating to execute a detection order addressed to it under this Regulation.

Or. en

Amendment 376

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 24

Text proposed by the Commission

(24) The competent judicial authority **or the competent independent administrative authority, as applicable in accordance with the detailed procedural rules set by the relevant Member State**, should be in a position to take a well-informed decision on requests for the issuance of detections orders. That is of particular importance to ensure the necessary fair balance of the fundamental rights at stake and a consistent approach, especially in connection to detection orders concerning the solicitation of children. Therefore, a procedure should be provided for that allows the providers concerned, the EU Centre on Child Sexual Abuse established by this Regulation ('EU Centre') and, **where so provided in this Regulation**, the competent data protection authority designated under Regulation (EU) 2016/679 to provide their views on the measures in question. They should do so **as soon as possible**, having regard to the important public policy objective at stake and the need to act **without undue delay** to

Amendment

(24) The competent judicial authority should **have the data necessary to** be in a position to take a well-informed decision on requests for the issuance of detections orders. That is of particular importance to ensure the necessary fair balance of the fundamental rights at stake and a consistent approach, especially in connection to detection orders concerning the solicitation of children. Therefore, a procedure should be provided for that allows the providers concerned, the EU Centre on Child Sexual Abuse established by this Regulation ('EU Centre') and the competent data protection authority designated under Regulation (EU) 2016/679 to provide their views on the measures in question, **as per Article 35 and 36 of that Regulation**. They should do so **without undue delay**, having regard to the important public policy objective at stake and the need to act to protect children. Furthermore, **data protection authorities** should normally be able to provide their opinion **in a timely manner**

protect children. *In particular, data protection authorities should do their utmost to avoid extending the time period set out in Regulation (EU) 2016/679 for providing their opinions in response to a prior consultation.* Furthermore, *they* should normally be able to provide their opinion *well within that time period* in situations where the European Data Protection Board has already issued guidelines regarding the technologies that a provider envisages deploying and operating to execute a detection order addressed to it under this Regulation.

including in situations where the European Data Protection Board has already issued guidelines regarding the technologies that a provider envisages deploying and operating to execute a detection order addressed to it under this Regulation.

Or. en

Amendment 377

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 25

Text proposed by the Commission

Amendment

(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,

deleted

as well as the overall remaining risk profile.

Or. en

Amendment 378
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 25

Text proposed by the Commission

Amendment

(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.

deleted

Or. en

Amendment 379
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 26

(26) *The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.* *deleted*

Or. en

Amendment 380
Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 26

Text proposed by the Commission

(26) ***The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.***

Amendment

(26) This Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures ***are not undermined***. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. ***Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting, circumventing or weakening end-to-end encryption.***

Or. en

Amendment 381

Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation

Recital 26

Text proposed by the Commission

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***That includes the use of*** end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

Amendment

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. End-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children, ***should be safeguarded. This includes no possibility within end-to-end encryption technology to build in so called ‘backdoors’, i.e. client-side scanning with side-channel leaks which could weaken the end-to-end encryption and lead to a third party getting access to private data. Client-side scanning, when a message is scanned twice, on sending and receiving, threatens the integrity and privacy of users. Such ‘backdoors’ should not be***

built in on end-to-end encryption in the pursuit of enforcing this regulation. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

Or. en

Amendment 382
Rob Rooken

Proposal for a regulation
Recital 26

Text proposed by the Commission

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, ***and avoid circumvention of the detection obligations,*** those measures should be ***taken regardless of*** the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the

Amendment

(26) The measures taken by providers of hosting services and providers of publicly available ***number independent*** interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, those measures should be ***tailored to*** the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end

requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an *important* tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

encryption technology, which is an *essential* tool to guarantee the security and confidentiality of the communications of users, including those of children. ***Detection orders should not under any circumstances be interpreted as prohibiting, weakening and breaking (including de facto) encryption or (including de facto) leading to the creation of any kind of backdoor.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users. ***If the provider reasonably believes that complying with a detection order will inevitably lead to undermining the security and confidentiality of the communications of its users, it should suspend its execution and challenge it in accordance with the procedure outlined in article 9.***

Or. en

Justification

Detection orders should be adapted to the service targeted and should not undermine the security or confidentiality of communication of its users.

Amendment 383

Sara Skyttedal, David Lega, Andrey Kovatchev, Tomáš Zdechovský, Stefan Berger, Christian Doleschal, Helmut Geuking, Ivan Štefanec, Peter Pollák, Johan Nissinen, Karen Melchior, Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari, Lukas Mandl, Rob Rooker

Proposal for a regulation **Recital 26**

Text proposed by the Commission

Amendment

(26) The measures taken by providers of

(26) The measures taken by providers of

hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***In accordance with Article 6a, nothing in this regulation shall be interpreted as prohibiting, or compromising the integrity and confidentiality of, end-to-end encrypted content or communications through client-side scanning with side-channel leaks or other measures by which the provider of a hosting service or a provider of interpersonal communication services provides third party actors with access to the end-to-end encrypted content and communications.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

Or. en

Justification

The integrity and confidentiality of end-to-end encrypted content and communications are essential for the confidentiality of digital correspondence and hence a prerequisite for the right to respect for private and family life and the right to protection of personal data as enshrined in Articles 7 and 8 of the Charter of the Fundamental Rights of the European Union (2000/C364/01). Client-side scanning with side-channel leaks is an example of a practice that, while not necessarily 'weakening' the end-to-end encryption, still puts the integrity and confidentiality of the end-to-end encrypted content and communications at risk.

Amendment 384

Jadwiga Wiśniewska

Proposal for a regulation

Recital 26

Text proposed by the Commission

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When

Amendment

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. **Nothing**

executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

in this Regulation should therefore be interpreted as prohibiting end-to-end encryption or making it impossible. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users, *while ensuring the effective detection of online child sexual abuse and the balance of all the fundamental rights at stake.*

Or. en

Amendment 385

Javier Moreno Sánchez, Juan Fernando López Aguilar, Domènec Ruiz Devesa, Pietro Bartolo, Hilde Vautmans, Antonio López-Istúriz White, Milan Brglez, Helène Fritzon, Estrella Durá Ferrandis, Evin Incir, Carina Ohlsson, Caterina Chinnici, Cyrus Engerer

Proposal for a regulation Recital 26

Text proposed by the Commission

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to

Amendment

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to

comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. ***Nothing in this Regulation should therefore be interpreted as prohibiting end-to-end encryption or making it impossible.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users, ***while ensuring the effective detection of online child sexual abuse and the balance of all the fundamental rights at stake.***

Or. en

Amendment 386
Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Recital 26

Text proposed by the Commission

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those

Amendment

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those

measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***Nothing in this Regulation should therefore be interpreted as prohibiting end-to-end encryption or making it impossible or leading to any form of general monitoring.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users. ***Under no circumstances should this Regulation be interpreted or used as an instrument of mass surveillance and monitoring.***

Or. en

Amendment 387
Carles Puigdemont i Casamajó

Proposal for a regulation
Recital 26

Text proposed by the Commission

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders

Amendment

(26) The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders

addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children.*** When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

Or. en

Amendment 388

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) Encryption is important to ensure the enjoyment of all human rights offline and online. Moreover, encryption technologies contribute in a fundamental way both to the respect for private life and confidentiality of communications, as well as to innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide. In the context of interpersonal communications, end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider. It should be noted that while E2EE is one of the most commonly used security measures in the context of electronic communications, other technical solutions (e.g., the use of other cryptographic schemes) might be or become equally important to secure and protect the confidentiality of digital communications. Thus, their use should not be prevented, circumvented or weakened either.

Or. en

Amendment 389

Sara Skyttedal, David Lega, Andrey Kovatchev, Tomáš Zdechovský, Stefan Berger, Christian Doleschal, Helmut Geuking, Ivan Štefanec, Peter Pollák, Johan Nissinen, Karen Melchior, Lukas Mandl, Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari, Rob Rooker

Proposal for a regulation Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) End-to-end encryption is an essential tool to guarantee the security, privacy and confidentiality of the communications between users, including

those of children. Any weakening of the end-to-end encryption's effect could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or compromising the integrity and confidentiality of end-to-end encrypted content and communications. As compromising the integrity of end-to-end encrypted content and communications shall be understood the processing of any data, that would compromise or put at risk the integrity and confidentiality of the aforementioned end-to-end encrypted content. Nothing in this regulation shall thus be interpreted as justifying client-side scanning with side-channel leaks or other measures by which the provider of a hosting service or a provider of interpersonal communication services provide third party actors access to the end-to-end encrypted content and communications.

Or. en

Justification

The integrity and confidentiality of end-to-end encrypted content and communications is essential for the confidentiality of digital correspondence and hence a prerequisite for the right to respect for private and family life and the right to protection of personal data as enshrined in Articles 7 and 8 of the Charter of the Fundamental Rights of the European Union (2000/C364/01). Client-side scanning with side-channel leaks is an example of a practice that, while not necessarily 'weakening' the end-to-end encryption, still puts the integrity and confidentiality of the end-to-end encrypted content and communications at risk.

Amendment 390

Carles Puigdemont i Casamajó

Proposal for a regulation

Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) End-to-end encryption is an important tool to guarantee the security and confidentiality of the communications

of users, including those of children. Any weakening of the end-to-end encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption. However, to the extent strictly necessary and proportionate to mitigate the risk of misuse of their services for the purpose of online child sexual abuse, providers should be authorised by the competent judicial authority or another independent administrative authority to process metadata that can detect suspicious patterns of behaviour without having access to the content of the encrypted communication.

Or. en

Amendment 391

Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation

Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) End-to-end encryption is vital for the security and privacy of the communications of users. The detection obligations set out in this regulation should therefore not apply to end-to-end encryption services, since it risks jeopardizing the integrity of such services. Consequently, the encryption should remain confidential without the possibility of side channel-leak mechanism built in from the service providers, which would endanger the privacy of users.

Or. en

Amendment 392

Rob Rooken

Proposal for a regulation
Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) *The act of ‘breaking’ encryption refers to the act of defeating or bypassing the encryption protocol used to secure a communication. Any access by any third-party that was not meant to access, read or edit the content of that communication that was supposed to be private and secure should be considered as bypassing encryption.*

Or. en

Amendment 393
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 26 b (new)

Text proposed by the Commission

Amendment

(26b) *The principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 applies to the technologies regulated by the Proposal by virtue of law.*

Or. en

Amendment 394
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 27

Text proposed by the Commission

Amendment

(27) *In order to facilitate the providers’ compliance with the detection obligations,* **deleted**

the EU Centre should make available to providers detection technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board should be consulted on those technologies and the ways in which they should be best deployed to ensure compliance with applicable rules of Union law on the protection of personal data. The advice of the European Data Protection Board should be taken into account by the EU Centre when compiling the lists of available technologies and also by the Commission when preparing guidelines regarding the application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

Or. en

Amendment 395

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 27

Text proposed by the Commission

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers **detection** technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board should be consulted on those technologies and the ways in which they should **be best** deployed **to ensure** compliance with applicable **rules of** Union law on the

Amendment

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board should be consulted on **the acceptability or otherwise of** those technologies and the ways in which they should **bet** deployed, **if at all, in** compliance with applicable Union law on

protection of personal data. The *advice* of the European Data Protection Board should be taken into account by the EU Centre *when compiling the lists of available technologies* and also by the Commission when preparing guidelines regarding the application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

the protection of personal data. The *authoritative position* of the European Data Protection Board should be *fully* taken into account by the EU Centre and also by the Commission when preparing guidelines regarding the application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation *and other applicable EU law, such as Regulation 2016/679. These technologies should be independently audited as regards their performance and reliability, and the benchmarks used as well as the results of the independent audit shall be made public.*

Or. en

Amendment 396
Annalisa Tardino

Proposal for a regulation
Recital 27

Text proposed by the Commission

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers detection technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board should be consulted on those technologies and the ways in which they should be best deployed to ensure compliance with applicable rules of Union law on the protection of personal data. The advice of the European Data Protection Board should be taken into account by the EU Centre when compiling the lists of available technologies and also by the Commission when preparing guidelines regarding the

Amendment

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers detection technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board should be consulted on *the use of* those technologies and the ways in which they should be best deployed to ensure compliance with applicable rules of Union law on the protection of personal data. The advice of the European Data Protection Board should be taken into account by the EU Centre when compiling the lists of available technologies and also by the Commission when preparing guidelines regarding the

application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

Or. en

Amendment 397

Tomas Tobé, Jessica Polfjärd, Jörgen Warborn, Arba Kokalari

Proposal for a regulation

Recital 27

Text proposed by the Commission

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers detection technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board **should** be consulted on those technologies and the ways in which they should be best deployed to ensure compliance with applicable rules of Union law on the protection of personal data. The advice of the European Data Protection Board **should** be taken into account by the EU Centre when compiling the lists of available technologies and also by the Commission when preparing guidelines regarding the application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

Amendment

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers detection technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board **must** be consulted on those technologies and the ways in which they should be best deployed to ensure compliance with applicable rules of Union law on the protection of personal data. The advice of the European Data Protection Board **must** be taken into account by the EU Centre when compiling the lists of available technologies and also by the Commission when preparing guidelines regarding the application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

Or. en

Amendment 398

Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 27 a (new)

Text proposed by the Commission

Amendment

(27a) *Since the consultation of the EDPB by the EU Center is a new task not foreseen under either Regulation 2016/679, Regulation 2018/1725 or Directive 2016/680, the EDPB budget and staffing should be adapted accordingly. The situation of national authorities, who too will be regularly consulted by service providers, should also reflect their increased responsibilities.*

Or. en

Amendment 399
René Repasi, Tiemo Wölken
on behalf of the S&D Group
Petar Vitanov
on behalf of the Committee on Civil Liberties, Justice and Home Affairs
Birgit Sippel

Proposal for a regulation
Recital 27 a (new)

Text proposed by the Commission

Amendment

(27a) *The Commission shall ensure in the draft general budget of the Union that the European Data Protection Board and European Data Protection Supervisor are provided with sufficient human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers pursuant to this Regulation.*

Or. en

Amendment 400

Fabienne Keller, Nathalie Loiseau

Proposal for a regulation

Recital 27 a (new)

Text proposed by the Commission

Amendment

(27a) Due to the nature of child sexual abuse materials, the sharing of those contents does not stop at border. The competent authorities and the EU Centre should therefore have a cooperation procedure with the American NCMEC (The National Center for Missing and Exploited Children) to detect and remove those contents more effectively.

Or. en

Amendment 401

Javier Moreno Sánchez, Juan Fernando López Aguilar, Domènec Ruiz Devesa, Pietro Bartolo, Hilde Vautmans, Antonio López-Istúriz White, Milan Brglez, Helène Fritzon, Estrella Durá Ferrandis, Evin Incir, Carina Ohlsson, Caterina Chinnici, Cyrus Engerer

Proposal for a regulation

Recital 27 a (new)

Text proposed by the Commission

Amendment

(27a) To the extent strictly necessary and proportionate to mitigate the risk of misuse of their services for the purpose of online child sexual abuse, it should be possible for the Coordinating Authority of establishment to authorise providers to process metadata.

Or. en

Amendment 402

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 28

Text proposed by the Commission

Amendment

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, as well as to identify false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children.

deleted

Or. en

Amendment 403

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 28

Text proposed by the Commission

Amendment

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently **reliable**, as well as to identify false positives and avoid **to the extent** erroneous reporting to the EU Centre, **providers** should ensure human oversight and, where

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently **accurate**, as well as to identify false positives and **false negatives and to** avoid erroneous reporting to the EU Centre, **law enforcement** should ensure **adequate**

necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. ***In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children.***

human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples ***forwarded by providers.***

Or. en

Justification

It is absolutely not the role of non-specialised staff of private companies to analyse the communications of private individuals and to guess their motivations.

Amendment 404

Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation

Recital 28

Text proposed by the Commission

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, ***as well as to identify*** false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of

Amendment

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, ***do not produce too many*** false positives ***identifying the reasons for their appearance,*** and avoid to the extent erroneous reporting to the EU Centre, providers should ensure ***stringent*** human oversight and, where necessary ***and required to uphold the highest possible standards,*** human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular ***and***

anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children.

independent assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children.

Or. en

Amendment 405
Annalisa Tardino

Proposal for a regulation
Recital 28

Text proposed by the Commission

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, as well as to identify false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential

Amendment

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, as well as to identify false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential

solicitation of children.

solicitation of children. ***Providers should ensure that staff carrying out such task is adequately trained.***

Or. en

Amendment 406
Rob Rooker

Proposal for a regulation
Recital 28

Text proposed by the Commission

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, as well as to identify false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children.

Amendment

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently reliable, as well as to identify false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and positives generated by the technologies, based on an analysis of anonymised representative data samples. In particular where the detection of the solicitation of children in publicly available ***number independent*** interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children.

Or. en

Amendment 407
Jadwiga Wiśniewska

Proposal for a regulation

Recital 29

Text proposed by the Commission

(29) Providers of hosting services and providers of publicly available interpersonal communications services are uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report on potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are reasonable grounds to believe that a particular activity may constitute online child sexual abuse. Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative. Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

Amendment

(29) Providers of hosting services and providers of publicly available interpersonal communications services are uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report on potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are reasonable grounds to believe that a particular activity may constitute online child sexual abuse. ***In such a case, hosting providers and providers of publicly available interpersonal communication services should be required to secure the disclosed child sexual abuse material and any metadata they hold about that material, including metadata which may indicate the author of the file, the time and circumstances of its creation and the modifications made.***

Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest

against child sexual abuse, or activities conducted on the providers' own initiative. Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them. ***In the event of an investigation, providers should provide any electronic evidence in their possession, as indicated above, upon request by law enforcement authorities.***

Or. en

Amendment 408
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 29

Text proposed by the Commission

(29) Providers of hosting services and providers of publicly available interpersonal communications services ***are uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they*** should be required to report on potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are ***reasonable*** grounds to believe that a particular activity may constitute online child sexual abuse. ***Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports.*** In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness

Amendment

(29) Providers of hosting services and providers of publicly available ***number independent*** interpersonal communications services should be required to report on potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are ***serious*** grounds to believe that a particular activity may constitute online child sexual abuse. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness could, for example, be obtained through information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative. ***Wherever possible,*** those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where

could, for example, be obtained through ***the execution of detection orders***, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative. Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

relevant, and should ensure that the reports are as complete as possible before submitting them.

Or. en

Amendment 409
Rob Rooken

Proposal for a regulation
Recital 29

Text proposed by the Commission

(29) Providers of hosting services and providers of publicly available interpersonal communications services ***are uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report on potential*** online child sexual abuse on their services, whenever they become aware of it, that is, when there are ***reasonable*** grounds to believe that a particular activity may constitute online child sexual abuse. ***Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports.*** In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness

Amendment

(29) Providers of hosting services and providers of publicly available ***number independent*** interpersonal communications services should report on online child sexual abuse on their services, whenever they become aware of it, that is, when there are ***serious*** grounds to believe that a particular activity may constitute online child sexual abuse. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative. ***Wherever possible***, those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation,

could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative. Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

where relevant, and should ensure that the reports are as complete as possible before submitting them.

Or. en

Justification

Recital 29 goes very far legally, requiring providers of interpersonal communications services to report even on "potential" instances of CSA, suggesting that all providers should proactively "detect" such content. Such requirements seem to be too far reaching. Changes are introduced to make sure that the recital remains proportionate and to ensure efficient protection of users' fundamental rights.

Amendment 410

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 29

Text proposed by the Commission

(29) ***Providers of hosting services and providers of publicly available interpersonal communications services are uniquely positioned to detect potential online child sexual abuse involving their services.*** The information ***that they*** may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report ***on*** potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are

Amendment

(29) The information ***providers*** may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are reasonable grounds to believe that a particular activity may constitute online child sexual abuse. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness.

reasonable grounds to believe that a particular activity may constitute online child sexual abuse. *Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports.* In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. *Such awareness could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative.* Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

However, nothing in this Regulation should be interpreted as providing for a legal basis for the processing of personal data for the sole purpose of detecting online child sexual abuse on a voluntary basis where a detection order has not been issued. Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

Or. en

Justification

The first deleted sentence is demonstrably false.

The second deleted sentence creates unnecessary confusion as to what "reasonable grounds" means.

The third deleted sentence unnecessarily explains "immaterial", whose meaning is entirely clear.

Amendment 411 **Vincenzo Sofo, Jadwiga Wiśniewska**

Proposal for a regulation **Recital 29**

Text proposed by the Commission

(29) Providers of hosting services and providers of publicly available interpersonal communications services are

Amendment

(29) Providers of hosting services and providers of publicly available interpersonal communications services are

uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report on potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are reasonable grounds to believe that a particular activity may constitute online child sexual abuse. Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. *Such awareness could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative.* Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report on potential online child sexual abuse on their services, whenever they become aware of it, that is, when there are reasonable grounds to believe that a particular activity may constitute online child sexual abuse. Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. *The providers can obtain such actual knowledge or awareness, inter alia, through its own initiative investigations, as well as through information flagged or notified by users, self-reported by victims or organizations, such as hotlines, acting in the public interest against child sexual abuse.* Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them *so that competent law enforcement authorities can focus on reports that are most likely to lead to recovery of a child, the arrest of an offender, or both.*

Or. en

Amendment 412
Jadwiga Wiśniewska

Proposal for a regulation
Recital 29 a (new)

(29a) It is also crucial that hosting providers and providers of publicly available interpersonal communication services cooperate with law enforcement in relation to the detection of potential online child abuse and the possession of key electronic evidence necessary for the proper prosecution of child sexual abuse cases. Therefore, in order to ensure the effective use of secured child sexual abuse material, it is necessary to legally ensure that providers secure not only the media files and instant messaging content themselves, but also their metadata. Metadata is information about documents/files relating to their content, technical and physical parameters. It also includes information such as the time and place of their creation, information about the devices used in their creation, and about the modifications made to the files. It is reasonable to expect service providers, in the event of the disclosure of child sexual abuse content, to secure it and then hand over, at the request of law enforcement authorities, any data indicated above that constitute electronic evidence in the case. It should be stressed that metadata can constitute important evidence, which will be important for law enforcement in the course of an investigation, and its ephemeral and easily modifiable nature requires it to be secured immediately, as it can contribute to the identification not only of the perpetrator and other persons linked to the uploaded content, but also of the victims

Or. en

Amendment 413
Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation

Recital 30

Text proposed by the Commission

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Amendment

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection. ***Any removal or disabling of access should respect the fundamental rights of the users of the service, including the right to freedom of expression and of information.*** Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Or. en

Amendment 414

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 30

Text proposed by the Commission

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial ***authorities or independent administrative*** authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may

Amendment

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided

affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences. ***Users should be notified in any case whenever a report concerning them is submitted by the EU Center to a competent national authority, in order to be able to exercise their right of redress.***

Or. en

Amendment 415
Annalisa Tardino

Proposal for a regulation
Recital 30

Text proposed by the Commission

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Amendment

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection ***and in order to stop or limit its dissemination***, Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Or. en

Amendment 416
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 30

Text proposed by the Commission

(30) To ensure that online child sexual abuse material is removed as swiftly as possible ***after its detection***, Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal ***or disabling of access*** may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Amendment

(30) To ensure that online child sexual abuse material is removed as swiftly as possible. Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Or. en

Amendment 417
Maite Pagazaurtundúa, Moritz Körner

Proposal for a regulation
Recital 30

Text proposed by the Commission

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial ***authorities or independent administrative*** authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided

Amendment

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should

the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Or. en

Amendment 418
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 32

Text proposed by the Commission

Amendment

(32) The obligations of this Regulation do not apply to providers of hosting services that do not offer their services in the Union. However, such services may still be used to disseminate child sexual abuse material to or by users in the Union, causing harm to children and society at large, even if the providers' activities are not targeted towards Member States and the total numbers of users of those services in the Union are limited. For legal and practical reasons, it may not be reasonably possible to have those providers remove or disable access to the material, not even through cooperation with the competent authorities of the third country where they are established. Therefore, in line with existing practices in several Member States, it should be possible to require providers of internet access services to take reasonable measures to block the access of users in the Union to the material.

deleted

Or. en

Amendment 419

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 32

Text proposed by the Commission

(32) The obligations of this Regulation do not apply to providers of hosting services that do not offer their services in the Union. However, such services may still be used to disseminate child sexual abuse material to or by users in the Union, causing harm to children and society at large, even if the providers' activities are not targeted towards Member States and the total numbers of users of those services in the Union are limited. ***For legal and practical reasons, it may not be reasonably possible to have those providers remove or disable access to the material, not even through cooperation with the competent authorities of the third country where they are established. Therefore, in line with existing practices in several Member States, it should be possible to require providers of internet access services to take reasonable measures to block the access of users in the Union to the material.***

Amendment

(32) The obligations of this Regulation do not apply to providers of hosting services that do not offer their services in the Union. However, such services may still be used to disseminate child sexual abuse material to or by users in the Union, causing harm to children and society at large, even if the providers' activities are not targeted towards Member States and the total numbers of users of those services in the Union are limited. ***As every country in the world has ratified either the UN Convention on the Rights of the Child or its optional Protocol on Child Pornography, it should always be possible to have those providers remove or disable access to the material. Where problems arise in relation to specific jurisdictions, all possible diplomatic pressure should be brought to bear by the Commission and Member States to remedy the situation.***

Or. en

Amendment 420

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 33

Text proposed by the Commission

(33) ***In the interest of consistency, efficiency and effectiveness and to minimise the risk of circumvention, such***

Amendment

deleted

blocking orders should be based on the list of uniform resource locators, leading to specific items of verified child sexual abuse, compiled and provided centrally by the EU Centre on the basis of diligently verified submissions by the relevant authorities of the Member States. In order to avoid the taking of unjustified or disproportionate measures, especially those that would unduly affect the fundamental rights at stake, notably, in addition to the rights of the children, the users' freedom of expression and information and the providers' freedom to conduct a business, appropriate limits and safeguards should be provided for. In particular, it should be ensured that the burdens imposed on the providers of internet access services concerned are not unreasonable, that the need for and proportionality of the blocking orders is diligently assessed also after their issuance and that both the providers and the users affected have effective means of judicial as well as non-judicial redress.

Or. en

Amendment 421
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 33

Text proposed by the Commission

Amendment

(33) *In the interest of consistency, efficiency and effectiveness and to minimise the risk of circumvention, such blocking orders should be based on the list of uniform resource locators, leading to specific items of verified child sexual abuse, compiled and provided centrally by the EU Centre on the basis of diligently verified submissions by the relevant authorities of the Member States. In order to avoid the taking of unjustified or*

deleted

disproportionate measures, especially those that would unduly affect the fundamental rights at stake, notably, in addition to the rights of the children, the users' freedom of expression and information and the providers' freedom to conduct a business, appropriate limits and safeguards should be provided for. In particular, it should be ensured that the burdens imposed on the providers of internet access services concerned are not unreasonable, that the need for and proportionality of the blocking orders is diligently assessed also after their issuance and that both the providers and the users affected have effective means of judicial as well as non-judicial redress.

Or. en

Amendment 422
Annalisa Tardino

Proposal for a regulation
Recital 35

Text proposed by the Commission

(35) *The* dissemination of child sexual abuse material is a criminal offence that affects the rights of the victims depicted. Victims should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation.

Amendment

(35) *Any* dissemination of child sexual abuse **material, including the non-consensual dissemination of self-generated** material is a criminal offence that affects the rights of the victims depicted. **Repeated dissemination of child sexual abuse material constitutes a form of revictimisation which could cause long-lasting negative consequences on the victim.** Victims should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation. **Staff dealing with such cases shall be**

specifically trained to interact with victims of serious abuse.

Or. en

Amendment 423

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 35

Text proposed by the Commission

(35) The dissemination of child sexual abuse material is a criminal offence that affects the rights of the *victims* depicted. *Victims* should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation.

Amendment

(35) The dissemination of child sexual abuse material is a criminal offence that affects the rights of the *survivors* depicted. *Survivors* should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation ***and have the right to request the deletion of this child sexual abuse material. In such a case, survivors should have the right to obtain relevant information, upon request, from the EU Centre via the Coordinating Authorities.***

Or. en

Amendment 424

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 35

Text proposed by the Commission

(35) The dissemination of child sexual abuse material is a criminal offence that

Amendment

(35) The dissemination of child sexual abuse material is a criminal offence that

affects the rights of the victims depicted. Victims should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation.

affects the rights of the victims depicted. Victims *or their approved formal representative* should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported *or has been removed* by providers of hosting services or providers of publicly available *number-independent* interpersonal communications services in accordance with this Regulation.

Or. en

Amendment 425
Rob Rooker

Proposal for a regulation
Recital 35

Text proposed by the Commission

(35) The dissemination of child sexual abuse material is a criminal offence that affects the rights of the victims depicted. Victims should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation.

Amendment

(35) The dissemination of child sexual abuse material is a criminal offence that affects the rights of the victims depicted. Victims should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available *number independent* interpersonal communications services in accordance with this Regulation.

Or. en

Amendment 426
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 35 a (new)

(35a) As pointed out in the Commission Strategy ^{1a}, children themselves need to have the knowledge and tools that could help them not to be confronted with the abuse when possible and they need to be informed that certain behaviours are not acceptable. The Commission-funded network of Safer Internet Centres raises awareness on online safety and provides information, resources and assistance via helplines and hotlines on a wide range of digital safety topics including grooming and sexting. The One in Five campaign by the Council of Europe and Europol’s “#SayNo” initiative are further examples of how this can be done. When abuse occurs, children need to feel secure and empowered to speak up, react and report, even when the abuse comes from within their circle of trust, as it is often the case. They also need to have access to safe, accessible and age-appropriate channels to report the abuse without fear. As stated in the Recommendation of the UN Committee on the Rights of the Child ^{1b}, state parties should ensure that digital literacy is taught in schools, as part of basic education curricula, from the preschool level and throughout all school years, and that such pedagogies are assessed on the basis of their results. Curricula should include the knowledge and skills to safely handle a wide range of digital tools and resources, including those relating to content, creation, collaboration, participation, socialization and civic engagement EU strategy for a more effective fight against child sexual abuse.

^{1a} COM(2020) 607 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions EU strategy for

a more effective fight against child sexual abuse

^{1b} CRC/C/GC/25 , General comment No. 25 (2021) on children's rights in relation to the digital environment from UN Committee on the Rights of the Child

Or. en

Amendment 427

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 36

Text proposed by the Commission

(36) Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims who request the removal or disabling of access of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to be assisted by the EU Centre in this regard, via the Coordinating Authorities.

Amendment

(36) *In order to prevent children falling victim to online abuse, providers for which there is evidence that their service is routinely or systematically used for the purpose of online child sexual abuse should provide reasonable assistance, by putting in place alert and alarm mechanisms in a prominent way on their platforms. The alert mechanism could consist of, for example, linking potential victims to the local services such as helplines, victims' rights and support organisations or hotlines. They should ensure adequate follow-up, when a report or alert is made, in the language chosen by the user for using their service.* Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims who request the removal or disabling of access of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to

factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to *receive adequate psycho-social, child friendly and gender-sensitive support and to be assisted by the EU Centre and its relevant partners, such as child helplines or other psycho-social support mechanisms* in this regard, via the Coordinating Authorities. *Member States should establish and improve the functioning of child helplines and hotlines, including through funding and capacity building, in line with article 96 of Directive (EU) 2018/1972. Victim identification is key not only for tracking down online child sexual abuse but also to prevent victimisation, and to stop further spread of damaging material and to ensure that victims can benefit from available assistance. Such victim identification however, requires a high degree of specialisation and adequate resources. Therefore the European Cybercrime Centre's efforts in victim identification should be complemented at national level.*

Or. en

Amendment 428

Lucia Ďuriš Nicholsonová, Fabienne Keller

Proposal for a regulation

Recital 36

Text proposed by the Commission

Amendment

(36) Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims who request the removal or disabling of access of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to be assisted by the EU Centre in this regard, via the Coordinating Authorities.

(36) Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims who request the removal or disabling of access of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to be assisted by the EU Centre in this regard, via the Coordinating Authorities. ***Providers should create and run an accessible, age-appropriate and user-friendly mechanism allowing users to flag any instances of potential online child sexual abuse on their platform. The providers should also offer reasonable assistance to the users who report these cases, such as implementing visible alert and alarm systems on their platforms, as well as providing links to local organizations such as hotlines, helplines, or victims' rights organizations, to assist potential victims.***

Or. en

Amendment 429
Annalisa Tardino

Proposal for a regulation

Recital 36

Text proposed by the Commission

(36) Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims who request the removal or disabling of access of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to be assisted by *the* EU Centre in this regard, via the Coordinating Authorities.

Amendment

(36) Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims *or their legal representatives* who request the removal or disabling of access of the material in question. That assistance should *be user friendly and* remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to be assisted by *specifically trained* EU Centre *staff* in this regard, via the Coordinating Authorities.

Or. en

Amendment 430

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 36

Text proposed by the Commission

(36) Given the impact on the rights of *victims* depicted in such known child sexual abuse material and the typical

Amendment

(36) Given the impact on the rights of *survivors* depicted in such known child sexual abuse material and the typical

ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist **victims** who request the removal **or disabling of access** of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing **or disabling access to** the items. Considering that carrying out the activities needed to obtain such removal **or disabling of access** can be painful or even traumatic as well as complex, **victims** should also have the right to be assisted by the EU Centre in this regard, via the Coordinating Authorities.

ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist **survivors** who request the removal of the material in question **in a timely manner, in order to minimise the impact that such offences have on the physical and mental health of the minor**. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing the items. Considering that carrying out the activities needed to obtain such removal can be painful or even traumatic as well as complex, **survivors** should also have the right **to receive adequate support and** to be assisted by the EU Centre in this regard, via the Coordinating Authorities.

Or. en

Amendment 431
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 37

Text proposed by the Commission

(37) To ensure the efficient management of such **victim** support functions, **victims** should be allowed to contact and rely on the Coordinating Authority that is most accessible to them, which should channel all communications between **victims** and the EU Centre.

Amendment

(37) To ensure the efficient management of such **survivor** support functions, **survivors** should **be informed about the existence of such functions and** be allowed to contact and rely on the Coordinating Authority that is most accessible to them, which should channel all communications between **survivors** and the EU Centre.

Amendment 432
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 38

Text proposed by the Commission

(38) For the purpose of facilitating the exercise of the *victims*' right to information and of assistance and support for removal *or disabling of access*, *victims* should be allowed to indicate the relevant item or items of child sexual abuse material in respect of which they are seeking to obtain information or removal *or disabling of access* either by means of providing the image or images or the video or videos themselves, or by means of providing the uniform resource locators leading to the specific item or items of child sexual abuse material, or by means of any other representation allowing for the unequivocal identification of the item or items in question.

Amendment

(38) For the purpose of facilitating the exercise of the *survivors*' right to information and of assistance and support for removal, *survivors* should be allowed to indicate the relevant item or items of child sexual abuse material in respect of which they are seeking to obtain information or removal either by means of providing the image or images or the video or videos themselves, or by means of providing the uniform resource locators leading to the specific item or items of child sexual abuse material, or by means of any other representation allowing for the unequivocal identification of the item or items in question.

Amendment 433
Lucia Ďuriš Nicholsonová

Proposal for a regulation
Recital 44

Text proposed by the Commission

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one

Amendment

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one

lead authority as the Coordinating Authority, whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of other national authorities.

lead authority as the Coordinating Authority, whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of other national authorities. ***The Coordinating Authority should oversee the implementation of the Regulation, including issues related to prevention, education and awareness raising, and organise and promote regular trainings for officials, including law enforcement authorities, who deal with cases which involve children.***

Or. en

Amendment 434
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 44

Text proposed by the Commission

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one lead authority as the Coordinating Authority, whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of

Amendment

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one lead authority as the Coordinating Authority, whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of

other national authorities.

other national authorities. ***The Coordinating Authority should oversee issues related to prevention, education and awareness raising, and organise and promote regular trainings for officials, including law enforcement authorities, who deal with cases which involve children.***

Or. en

Amendment 435
Annalisa Tardino

Proposal for a regulation
Recital 44

Text proposed by the Commission

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one lead authority as the Coordinating Authority, ***whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority.*** For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of other national authorities.

Amendment

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one lead authority as the Coordinating Authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of other national authorities.

Or. en

Amendment 436
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 48

Text proposed by the Commission

(48) Given the need to ensure the effectiveness of the obligations imposed, Coordinating Authorities should be granted enforcement powers to address infringements of this Regulation. ***These powers should include the power to temporarily restrict access of users of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider on which the infringement takes place. In light of the high level of interference with the rights of the service providers that such a power entails, the latter should only be exercised when certain conditions are met. Those conditions should include the condition that the infringement results in the regular and structural facilitation of child sexual abuse offences, which should be understood as referring to a situation in which it is apparent from all available evidence that such facilitation has occurred on a large scale and over an extended period of time.***

Amendment

(48) Given the need to ensure the effectiveness of the obligations imposed, Coordinating Authorities should be granted enforcement powers to address infringements of this Regulation.

Or. en

Amendment 437

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 49

Text proposed by the Commission

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders, removal ***orders or blocking*** orders that it issued, are effectively complied ***in practice***, each Coordinating Authority should be able to carry out ***searches, using the*** relevant

Amendment

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders ***or*** removal orders that it issued, are effectively complied ***with***, each Coordinating Authority should be able to carry out relevant ***searches***.

indicators provided by the EU Centre, to detect the dissemination of known or new child sexual abuse material through publicly available material in the hosting services of the providers concerned.

Or. en

Amendment 438

Lucia Ďuriš Nicholsonová, Fabienne Keller

Proposal for a regulation

Recital 49

Text proposed by the Commission

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders, removal orders or blocking orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, using the relevant indicators provided by the EU Centre, to detect the dissemination of known or new child sexual abuse material through publicly available material in the hosting services of the providers concerned.

Amendment

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders, removal orders or blocking orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, using the relevant indicators provided by the EU Centre, **and reacting timely to the evolving trends of child sexual abuse material dissemination and monetisation**, to detect the dissemination of known or new child sexual abuse material through publicly available material in the hosting services of the providers concerned.

Or. en

Amendment 439

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 49

Text proposed by the Commission

(49) In order to verify that the rules of this Regulation, in particular those on

Amendment

(49) In order to verify that the rules of this Regulation, in particular those on

mitigation measures and ***on the execution of detection orders, removal orders or blocking orders*** that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, ***using the relevant indicators provided by the EU Centre***, to detect the dissemination of known ***or new*** child sexual abuse material through publicly available material in the hosting services of the providers concerned.

mitigation measures and, removal orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, to detect the dissemination of known child sexual abuse material through publicly available material in the hosting services of the providers concerned.

Or. en

Amendment 440
Carles Puigdemont i Casamajó

Proposal for a regulation
Recital 49

Text proposed by the Commission

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders, removal ***orders or*** blocking orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, using the relevant indicators provided by the EU Centre, to detect the dissemination of known or new child sexual abuse material through publicly available material in the hosting services of the providers concerned.

Amendment

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of ***voluntary*** detection orders, ***detection,*** removal, blocking ***or delisting*** orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, using the relevant indicators provided by the EU Centre, to detect the dissemination of known or new child sexual abuse material through publicly available material in the hosting services of the providers concerned.

Or. en

Amendment 441
Carles Puigdemont i Casamajó

Proposal for a regulation
Recital 49 a (new)

(49a) Detection orders, which would require communication service providers to monitor their users' online activities for the purpose of detecting child sexual abuse material (CSAM), should only be imposed as a last resort in cases where a provider is found to be acting in bad faith and failing to cooperate with competent authorities. The use of detection orders should be proportionate, necessary, and subject to strict safeguards, and should only be authorized by a judicial authority or other independent oversight body. In any case, users should not be punished for merely using a communication service, and any measures taken to detect or remove CSAM should be implemented in a manner that respects users' privacy and other fundamental rights.

Or. en

Amendment 442

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 50

Text proposed by the Commission

(50) With a view to ensuring that providers of hosting services are aware of the misuse made of their services and to **afford them an opportunity** to take expeditious action to remove or disable access **on a voluntary basis**, Coordinating Authorities of establishment should be able to notify those providers of the presence of known child sexual abuse material on their services and **requesting** removal or disabling of access thereof, **for the providers' voluntary consideration. Such notifying activities should be clearly distinguished from the Coordinating**

Amendment

(50) With a view to ensuring that providers of hosting services are aware of the misuse made of their services and to **require them** to take expeditious action to remove or disable access, Coordinating Authorities of establishment should be able to notify those providers of the presence of known child sexual abuse material on their services and **order** removal or disabling of access thereof.

Authorities’ powers under this Regulation to request the issuance of removal orders, which impose on the provider concerned a binding legal obligation to remove or disable access to the material in question within a set time period.

Or. en

Justification

If a coordinating body provides actual knowledge of known child sexual abuse material that is being disseminated by criminals on the services of a hosting service provider, removal should be obligatory and not “for the voluntary consideration” of the provider.

Amendment 443
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 50

Text proposed by the Commission

(50) With a view to ensuring that providers of hosting services are aware of the misuse made of their services and to afford them an opportunity to take expeditious action to remove ***or disable access*** on a voluntary basis, Coordinating Authorities of establishment should be able to notify those providers of the presence of known child sexual abuse material on their services and requesting removal ***or disabling of access*** thereof, for the providers’ voluntary consideration. Such notifying activities should be clearly distinguished from the Coordinating Authorities’ powers under this Regulation to request the issuance of removal orders, which impose on the provider concerned a binding legal obligation to remove ***or disable access to*** the material in question within a set time period.

Amendment

(50) With a view to ensuring that providers of hosting services are aware of the misuse made of their services and to afford them an opportunity to take expeditious action to remove on a voluntary basis, Coordinating Authorities of establishment should be able to notify those providers of the presence of known child sexual abuse material on their services and requesting removal thereof, for the providers’ voluntary consideration. Such notifying activities should be clearly distinguished from the Coordinating Authorities’ powers under this Regulation to request the issuance of removal orders, which impose on the provider concerned a binding legal obligation to remove the material in question within a set time period.

Or. en

Amendment 444
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 55

Text proposed by the Commission

Amendment

(55) It is essential for the proper functioning of the system of mandatory detection and blocking of online child sexual abuse set up by this Regulation that the EU Centre receives, via the Coordinating Authorities, material identified as constituting child sexual abuse material or transcripts of conversations identified as constituting the solicitation of children, such as may have been found for example during criminal investigations, so that that material or conversations can serve as an accurate and reliable basis for the EU Centre to generate indicators of such abuses. In order to achieve that result, the identification should be made after a diligent assessment, conducted in the context of a procedure that guarantees a fair and objective outcome, either by the Coordinating Authorities themselves or by a court or another independent administrative authority than the Coordinating Authority. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to new child sexual abuse material and the solicitation of children reported under this Regulation, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting.

deleted

Or. en

Amendment 445

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 55

Text proposed by the Commission

(55) It is essential for the proper functioning of ***the system of mandatory detection and blocking of online child sexual abuse set up by*** this Regulation that the EU Centre receives, via the Coordinating Authorities, material identified as constituting child sexual abuse material ***or transcripts of conversations identified as constituting the solicitation of children***, such as may have been found for example during criminal investigations, so that that material ***or conversations*** can serve as an accurate and reliable basis for the EU Centre to generate indicators of such abuses. In order to achieve that result, the identification should be made after a diligent assessment, conducted in the context of a procedure that guarantees a fair and objective outcome, either by the Coordinating Authorities themselves or by a court ***or another independent administrative authority than the Coordinating Authority***. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to new child sexual abuse material ***and the solicitation of children reported under this Regulation***, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting.

Amendment

(55) It is essential for the proper functioning of this Regulation that the EU Centre receives, via the Coordinating Authorities, material identified as constituting child sexual abuse material, such as may have been found for example during criminal investigations, so that that material can serve as an accurate and reliable basis for the EU Centre to generate indicators of such abuses. In order to achieve that result, the identification should be made after a diligent assessment, conducted in the context of a procedure that guarantees a fair and objective outcome, either by the Coordinating Authorities themselves or by a court. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to new child sexual abuse material, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting.

Or. en

Amendment 446

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Paul Tang, Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Recital 55

Text proposed by the Commission

(55) It is essential for the proper functioning of the system of mandatory detection **and blocking of online** child sexual abuse set up by this Regulation that the EU Centre receives, via the Coordinating Authorities, material identified as constituting child sexual abuse material **or transcripts of conversations identified as constituting the solicitation of children**, such as may have been found for example during criminal investigations, so that that material **or conversations** can serve as an accurate and reliable basis for the EU Centre to generate indicators of such abuses. In order to achieve that result, the identification should be made after a diligent assessment, conducted in the context of a procedure that guarantees a fair and objective outcome, either by the Coordinating Authorities themselves or by a court or another independent administrative authority than the Coordinating Authority. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to new child sexual abuse material **and the solicitation of children** reported under this Regulation, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting.

Amendment

(55) It is essential for the proper functioning of the system of mandatory detection **of** child sexual abuse set up by this Regulation that the EU Centre receives, via the Coordinating Authorities, material identified as constituting child sexual abuse material, such as may have been found for example during criminal investigations, so that that material can serve as an accurate and reliable basis for the EU Centre to generate indicators of such abuses. In order to achieve that result, the identification should be made after a diligent assessment, conducted in the context of a procedure that guarantees a fair and objective outcome, either by the Coordinating Authorities themselves or by a court or another independent administrative authority than the Coordinating Authority. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to new child sexual abuse material reported under this Regulation, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting.

Or. en

Amendment 447
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 55 a (new)

Text proposed by the Commission

Amendment

(55a) All communications containing illegal material should be encrypted to state of the art standards, all access by staff to such content should be limited to what is necessary and thoroughly logged. All such logs should be stored for a minimum of ten years.

Or. en

Amendment 448
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 56

Text proposed by the Commission

Amendment

(56) With a view to ensuring that the indicators generated by the EU Centre for the purpose of detection are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material or conversations to the attention of the Coordinating Authorities for those purposes.

deleted

Or. en

Amendment 449
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 56

Text proposed by the Commission

(56) With a view to ensuring that the indicators generated by the EU Centre **for the purpose of detection** are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material or conversations to the attention of the Coordinating Authorities for those purposes.

Amendment

(56) With a view to ensuring that the indicators generated by the EU Centre are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material or conversations to the attention of the Coordinating Authorities for those purposes.

Or. en

Amendment 450

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Paul Tang, Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation
Recital 56

Text proposed by the Commission

(56) With a view to ensuring that the indicators generated by the EU Centre for the purpose of detection are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material **or conversations** to the attention of the Coordinating Authorities for those purposes.

Amendment

(56) With a view to ensuring that the indicators generated by the EU Centre for the purpose of detection are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material to the attention of the Coordinating Authorities for those purposes.

Or. en

Amendment 451

Lucia Ďuriš Nicholsonová, Fabienne Keller

Proposal for a regulation

Recital 57

Text proposed by the Commission

(57) Certain providers of relevant information society services offer their services in several or even all Member States, whilst under this Regulation only a single Member State has jurisdiction in respect of a given provider. It is therefore imperative that the Coordinating Authority designated by the Member State having jurisdiction takes account of the interests of all users in the Union when performing its tasks and using its powers, without making any distinction depending on elements such as the users' location or nationality, and that Coordinating Authorities cooperate with each other in an effective and efficient manner. To facilitate such cooperation, the necessary mechanisms and information-sharing systems should be provided for. That cooperation shall be without prejudice to the possibility for Member States to provide for regular exchanges of views with other public authorities where relevant for the performance of the tasks of those other authorities and of the Coordinating Authority.

Amendment

(57) Certain providers of relevant information society services offer their services in several or even all Member States, whilst under this Regulation only a single Member State has jurisdiction in respect of a given provider. It is therefore imperative that the Coordinating Authority designated by the Member State having jurisdiction takes account of the interests of all users in the Union when performing its tasks and using its powers, without making any distinction depending on elements such as the users' location or nationality, and that Coordinating Authorities cooperate with each other in an effective and efficient manner. To facilitate such cooperation, the necessary mechanisms and information-sharing systems should be provided for. That cooperation shall be without prejudice to the possibility for Member States to provide for regular exchanges of views with other public authorities where relevant for the performance of the tasks of those other authorities and of the Coordinating Authority ***and receive reports concerning the trends in the dissemination and monetisation of child sexual abuse material from relevant organisations acting in the public interest against child sexual abuse and other stakeholders, including service providers.***

Or. en

Amendment 452

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 58

Text proposed by the Commission

(58) In particular, in order to facilitate the cooperation needed for the proper functioning of the mechanisms set up by this Regulation, the EU Centre should establish and maintain the necessary information-sharing systems. ***When establishing and maintaining such systems, the EU Centre should cooperate with the European Union Agency for Law Enforcement Cooperation ('Europol') and national authorities to build on existing systems and best practices, where relevant.***

Amendment

(58) In particular, in order to facilitate the cooperation needed for the proper functioning of the mechanisms set up by this Regulation, the EU Centre should establish and maintain the necessary information-sharing systems.

Or. en

Amendment 453

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 58

Text proposed by the Commission

(58) In particular, in order to facilitate the cooperation needed for the proper functioning of the mechanisms set up by this Regulation, the EU Centre should establish and maintain the necessary information-sharing systems. When establishing and maintaining such systems, the EU Centre should cooperate with the European Union Agency for Law Enforcement Cooperation ('Europol') and national authorities to build on existing systems and best practices, where relevant.

Amendment

(58) In particular, in order to facilitate the cooperation needed for the proper functioning of the mechanisms set up by this Regulation, the EU Centre should establish and maintain the necessary ***secure*** information-sharing systems. When establishing and maintaining such systems, the EU Centre should cooperate with the European Union Agency for Law Enforcement Cooperation ('Europol') and national authorities to build on existing systems and best practices, where relevant.

Or. en

Amendment 454

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 59

Text proposed by the Commission

(59) To support the implementation of this Regulation and contribute to the achievement of its objectives, the EU Centre should serve as a central facilitator, carrying out a range of specific tasks. The performance of those tasks requires strong guarantees of independence, in particular from law enforcement authorities, as well as a governance structure ensuring the effective, efficient and coherent performance of its different tasks, and legal personality to be able to interact effectively with all relevant stakeholders. Therefore, it should be established as a decentralised Union agency.

Amendment

(59) To support the implementation of this Regulation and contribute to the achievement of its objectives, the EU Centre should serve as a central facilitator, carrying out a range of specific tasks. The performance of those tasks requires strong guarantees of independence, in particular from law enforcement authorities, **including Europol**, as well as a governance structure ensuring the effective, efficient and coherent performance of its different tasks, and legal personality to be able to interact effectively with all relevant stakeholders. Therefore, it should be established as a decentralised Union agency.

Or. en

Amendment 455

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 60

Text proposed by the Commission

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of **the detection**, reporting **and blocking** obligations imposed on providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services. However, for that same reason,

Amendment

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of reporting obligations imposed on providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services. However, for that same reason, the EU Centre should also be charged with

the EU Centre should also be charged with certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of *or disabling of* access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of knowledge and expertise related to online child sexual abuse.

certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of knowledge and expertise related to online child sexual abuse.

Or. en

Amendment 456
Rob Rooken

Proposal for a regulation
Recital 60

Text proposed by the Commission

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of the detection, reporting and blocking obligations imposed on providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services. However, for that same reason, the EU Centre should also be charged with certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of or disabling of access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of knowledge and expertise related to online

Amendment

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of the detection, reporting and blocking obligations imposed on providers of hosting services, providers of publicly available *number independent* interpersonal communications services and providers of internet access services. However, for that same reason, the EU Centre should also be charged with certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of or disabling of access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of

child sexual abuse.

knowledge and expertise related to online child sexual abuse.

Or. en

Amendment 457

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 60

Text proposed by the Commission

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of the **detection, reporting and blocking** obligations imposed on providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services. However, for that same reason, the EU Centre should also be charged with certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of or disabling of access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of knowledge and expertise related to online child sexual abuse.

Amendment

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of the obligations imposed on providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services. However, for that same reason, the EU Centre should also be charged with certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of or disabling of access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of knowledge and expertise related to online child sexual abuse.

Or. en

Amendment 458

Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 61

Text proposed by the Commission

(61) The EU Centre should provide reliable information on which activities can reasonably be considered to constitute online child sexual abuse, so as to enable the detection and blocking thereof in accordance with this Regulation. Given the nature of child sexual abuse material, that reliable information needs to be provided without sharing the material itself. Therefore, the EU Centre should generate accurate and reliable indicators, based on identified child sexual abuse material and solicitation of children submitted to it by Coordinating Authorities in accordance with the relevant provisions of this Regulation. These indicators should allow technologies to detect the dissemination of either the same material (known material) or of different child sexual abuse material (new material), or the solicitation of children, as applicable.

Amendment

deleted

Or. en

Amendment 459
Lucia Ďuriš Nicholsonová

Proposal for a regulation
Recital 61

Text proposed by the Commission

(61) The EU Centre should provide reliable information on which activities can reasonably be considered to constitute online child sexual abuse, so as to enable the detection and blocking thereof in accordance with this Regulation. Given the nature of child sexual abuse material, that reliable information needs to be provided without sharing the material itself.

Amendment

(61) The EU Centre should provide reliable information on which activities can reasonably be considered to constitute online child sexual abuse, so as to enable the detection and blocking thereof in accordance with this Regulation. Given the nature of child sexual abuse material, that reliable information needs to be provided without sharing the material itself.

Therefore, the EU Centre should generate accurate and reliable indicators, based on identified child sexual abuse material and solicitation of children submitted to it by Coordinating Authorities in accordance with the relevant provisions of this Regulation. These indicators should allow technologies to detect the dissemination of either the same material (known material) or of different child sexual abuse material (new material), or the solicitation of children, as applicable.

Therefore, the EU Centre should generate accurate and reliable indicators, based on identified child sexual abuse material and solicitation of children submitted to it by Coordinating Authorities *or when appropriate, by the organisations acting in the public interest against child sexual abuse*, in accordance with the relevant provisions of this Regulation. These indicators should allow technologies to detect the dissemination of either the same material (known material) or of different child sexual abuse material (new material), or the solicitation of children, as applicable.

Or. en

Amendment 460
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 61 a (new)

Text proposed by the Commission

Amendment

(61a) The EU Centre should be charged with the provision of assistance to Coordinating Authorities, as well as the generation of research, prevention techniques and sharing of knowledge, best practices and expertise related to online child sexual abuse, successful initiatives on digital skills and competences in an age appropriate manner, including media literacy, on sex education, and reacting timely to the evolving trends of child sexual abuse material dissemination.

Or. en

Amendment 461
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 62

Text proposed by the Commission

(62) For the system established by this Regulation to function properly, the EU Centre should be charged with creating databases for each of those three types of online child sexual abuse, and with maintaining and operating those databases. For accountability purposes and to allow for corrections where needed, it should keep records of the submissions and the process used for the generation of the indicators.

Amendment

deleted

Or. en

Amendment 462
Rob Rooker

Proposal for a regulation
Recital 63

Text proposed by the Commission

(63) For the purpose of ensuring the traceability of the reporting process and of any follow-up activity undertaken based on reporting, as well as of allowing for the provision of feedback on reporting to providers of hosting services and providers of publicly available interpersonal communications services, generating statistics concerning reports and the reliable and swift management and processing of reports, the EU Centre should create a dedicated database of such reports. To be able to fulfil the above purposes, that database should also contain relevant information relating to those reports, such as the indicators representing the material and ancillary tags, which can indicate, for example, the fact that a reported image or video is part of a series of images and videos depicting the same

Amendment

(63) For the purpose of ensuring the traceability of the reporting process and of any follow-up activity undertaken based on reporting, as well as of allowing for the provision of feedback on reporting to providers of hosting services and providers of publicly available **number independent** interpersonal communications services, generating statistics concerning reports and the reliable and swift management and processing of reports, the EU Centre should create a dedicated database of such reports. To be able to fulfil the above purposes, that database should also contain relevant information relating to those reports, such as the indicators representing the material and ancillary tags, which can indicate, for example, the fact that a reported image or video is part of a series of images and videos depicting the same

victim or victims.

victim or victims.

Or. en

Amendment 463

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 63

Text proposed by the Commission

(63) For the purpose of ensuring the traceability of the reporting process and of any follow-up activity undertaken based on reporting, as well as of allowing for the provision of feedback on reporting to providers of hosting services and providers of publicly available interpersonal communications services, generating statistics concerning reports and the reliable and swift management and processing of reports, the EU Centre should create a dedicated database of such reports. To be able to fulfil the above purposes, that database should also contain relevant information relating to those reports, such as the indicators representing the material and ancillary tags, which can indicate, for example, the fact that a reported image or video is part of a series of images and videos depicting the same *victim or victims*.

Amendment

(63) For the purpose of ensuring the traceability of the reporting process and of any follow-up activity undertaken based on reporting, as well as of allowing for the provision of feedback on reporting to providers of hosting services and providers of publicly available interpersonal communications services, generating statistics concerning reports and the reliable and swift management and processing of reports, the EU Centre should create a dedicated database of such reports. To be able to fulfil the above purposes, that database should also contain relevant information relating to those reports, such as the indicators representing the material and ancillary tags, which can indicate, for example, the fact that a reported image or video is part of a series of images and videos depicting the same *survivor or survivors*.

Or. en

Amendment 464

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 64

Text proposed by the Commission

(64) Given the sensitivity of the data

Amendment

(64) Given the sensitivity of the data

concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of *indicators and databases of reports*, on the data contained therein and on their security. ***In particular, the data concerned should not be stored for longer than is strictly necessary. For the above reasons, access to the database of indicators should be given only to the parties and for the purposes specified in this Regulation, subject to the controls by the EU Centre, and be limited in time and in scope to what is strictly necessary for those purposes.***

concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of reports, on the data contained therein and on their security.

Or. en

Amendment 465
Annalisa Tardino

Proposal for a regulation
Recital 64

Text proposed by the Commission

(64) Given the sensitivity of the data concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of indicators and databases of reports, on the data contained therein and on their security. In particular, the data concerned should not be stored for longer than is strictly necessary. For the above reasons, access to the database of indicators should be given only to the parties and for the purposes specified in this Regulation, subject to the controls by the EU Centre, and be limited in time and in scope to what is strictly necessary for those purposes.

Amendment

(64) Given the sensitivity of the data concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of indicators and databases of reports, on the data contained therein and on their security. ***Such rules should be always handled by staff specifically trained for that purpose.*** In particular, the data concerned should not be stored for longer than is strictly necessary. For the above reasons, access to the database of indicators should be given only to the parties and for the purposes specified in this Regulation, subject to the controls by the EU Centre, and be limited in time and in scope to what is strictly necessary for those purposes.

Or. en

Amendment 466

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 65

Text proposed by the Commission

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU Centre should assess those reports in order to identify those that are **manifestly** unfounded, that is, where it is **immediately** evident, **without any** substantive legal **or** factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is **manifestly** unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

Amendment

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks **without receiving an overwhelming quantity of false positives**, reports should pass through the EU Centre. The EU Centre should **thoroughly** assess those reports in order to identify those that are unfounded, that is, where it is evident, **including after** substantive legal **and** factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

Or. en

Amendment 467

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 65

Text proposed by the Commission

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU Centre should assess those reports in order to identify those that are manifestly unfounded, that is, where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is manifestly unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

Amendment

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU Centre should assess those reports in order to identify those that are manifestly unfounded, that is, where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is manifestly unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available ***number independent*** interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

Or. en

Amendment 468
Rob Rooken

Proposal for a regulation
Recital 65

Text proposed by the Commission

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU

Amendment

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU

Centre should assess those reports in order to identify those that are manifestly unfounded, that is, where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is manifestly unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

Centre should assess those reports in order to identify those that are manifestly unfounded, that is, where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is manifestly unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available ***number independent*** interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

Or. en

Amendment 469

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 66

Text proposed by the Commission

(66) With a view to contributing to the effective application of this Regulation and the protection of victims' rights, the EU Centre should be able, upon request, to support victims and to assist Competent Authorities by conducting searches of hosting services for the dissemination of known child sexual abuse material that is publicly accessible, using the corresponding indicators. Where it identifies such material after having conducted such a search, the EU Centre should also ***be able to request*** the provider of the hosting service concerned ***to remove***

Amendment

(66) With a view to contributing to the effective application of this Regulation and the protection of victims' rights, the EU Centre should be able, upon request, to support victims and to assist Competent Authorities by conducting searches of hosting services for the dissemination of known child sexual abuse material that is publicly accessible, using the corresponding indicators. Where it identifies such material after having conducted such a search, the EU Centre should also ***send*** the provider of the hosting service concerned ***a notice of this***

or disable access to the item or items in question, given that the provider may not be aware of their presence and may be willing to do so on a voluntary basis.

manifestly illegal content.

Or. en

Amendment 470

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 66

Text proposed by the Commission

(66) With a view to contributing to the effective application of this Regulation and the protection of *victims*' rights, the EU Centre should be able, upon request, to support *victims* and to assist Competent Authorities by conducting searches of hosting services for the dissemination of known child sexual abuse material that is publicly accessible, *using the corresponding indicators*. Where it identifies such material after having conducted such a search, the EU Centre should also be able to request the provider of the hosting service concerned to *remove or disable access to* the item or items in question, given that the provider may not be aware of their presence and may be willing to do so on a voluntary basis.

Amendment

(66) With a view to contributing to the effective application of this Regulation and the protection of *survivors*' rights, the EU Centre should be able, upon request, to support *survivors* and to assist Competent Authorities by conducting searches of hosting services for the dissemination of known child sexual abuse material that is publicly accessible. Where it identifies such material after having conducted such a search, the EU Centre should also be able to request the provider of the hosting service concerned to the item or items in question, given that the provider may not be aware of their presence and may be willing to do so on a voluntary basis.

Or. en

Amendment 471

Lucia Ďuriš Nicholsonová

Proposal for a regulation

Recital 67

Text proposed by the Commission

(67) Given its central position resulting

Amendment

(67) Given its central position resulting

from the performance of its primary tasks under this Regulation and the information and expertise it can gather in connection thereto, the EU Centre should also contribute to the achievement of the objectives of this Regulation by serving as a hub for knowledge, expertise and research on matters related to the prevention and combating of online child sexual abuse. In this connection, the EU Centre should cooperate with relevant stakeholders from both within and outside the Union and allow Member States to benefit from the knowledge and expertise gathered, including best practices and lessons learned.

from the performance of its primary tasks under this Regulation and the information and expertise it can gather in connection thereto, the EU Centre should also contribute to the achievement of the objectives of this Regulation by serving as a hub for knowledge, expertise and research on matters related to the prevention and combating of online child sexual abuse, ***including on the successful initiatives and good practices on the proactive search for online child sexual material, trends in its creation and monetisation, as well as the voluntary prevention, detection and mitigation of online child sexual abuse.*** In this connection, the EU Centre should cooperate with relevant stakeholders from both within and outside the Union and allow Member States to benefit from the knowledge and expertise gathered, including best practices and lessons learned.

Or. en

Amendment 472
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 67

Text proposed by the Commission

(67) Given its central position resulting from the performance of its primary tasks under this Regulation and the information and expertise it can gather in connection thereto, the EU Centre should also contribute to the achievement of the objectives of this Regulation by serving as a hub for knowledge, expertise and research on matters related to the prevention and combating of online child sexual abuse. In this connection, the EU Centre should cooperate with relevant stakeholders ***from both within and outside***

Amendment

(67) Given its central position resulting from the performance of its primary tasks under this Regulation and the information and expertise it can gather in connection thereto, the EU Centre should also contribute to the achievement of the objectives of this Regulation by serving as a hub for knowledge, expertise and research on matters related to the prevention and combating of online child sexual abuse, ***including lessons learned from, prevention and awareness raising campaigns.*** In this connection, the EU

the Union and allow Member States to benefit from the knowledge and expertise gathered, including best practices and lessons learned.

Centre should cooperate with relevant stakeholders and allow Member States to benefit from the knowledge and expertise gathered, including best practices and lessons learned ***on creating safe digital experiences for children and promoting their empowerment and active participation in the digital environment.***

Or. en

Amendment 473

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 68

Text proposed by the Commission

(68) Processing and storing certain personal data is necessary for the performance of the EU Centre's tasks under this Regulation. In order to ensure that such personal data is adequately protected, the EU Centre should only process and store personal data if strictly necessary for the purposes detailed in this Regulation. It should do so in a secure manner and limit storage to what is strictly necessary for the performance of the relevant tasks.

Amendment

(68) Processing and storing certain personal data is necessary for the performance of the EU Centre's tasks under this Regulation. In order to ensure that such personal data is adequately protected, the EU Centre should only process and store personal data if strictly necessary for the purposes detailed in this Regulation. It should do so in a secure manner, ***use state of the art encryption,*** and limit storage to what is strictly necessary for the performance of the relevant tasks. ***It should ensure adequate protection of its infrastructure and implement facilities access control, storage control, user control, control of data entry, data access control, communication control, input control, transport control, personnel profiles procedures, incident and recovery procedures, and ensure the reliability and integrity of its databases.***

Or. en

Amendment 474
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 69

Text proposed by the Commission

(69) In order to allow for the effective and efficient performance of its tasks, the EU Centre should closely cooperate with Coordinating Authorities, **the Europol** and relevant partner organisations, such as the US National Centre for Missing and Exploited Children or the International Association of Internet Hotlines ('INHOPE') network of hotlines for reporting child sexual abuse material, within the limits sets by this Regulation and other legal instruments regulating their respective activities. To facilitate such cooperation, the necessary arrangements should be made, including the designation of contact officers by Coordinating Authorities and the conclusion of **memoranda of understanding** with Europol and, where appropriate, with one or more of the relevant partner organisations.

Amendment

(69) In order to allow for the effective and efficient performance of its tasks, the EU Centre should closely cooperate with Coordinating Authorities, and relevant partner organisations, such as the US National Centre for Missing and Exploited Children or the International Association of Internet Hotlines ('INHOPE') network of hotlines for reporting child sexual abuse material, within the limits sets by this Regulation and other legal instruments regulating their respective activities. To facilitate such cooperation, the necessary arrangements should be made, including the designation of contact officers by Coordinating Authorities and the conclusion of **a working arrangement** with Europol and, where appropriate, with one or more of the relevant partner organisations.

Or. en

Amendment 475
Annalisa Tardino

Proposal for a regulation
Recital 69 a (new)

Text proposed by the Commission

Amendment

(69a) In order to strenghten prevention measures, the EU Centre shall cooperate with relevant national authorities to identify possible new patterns regarding child sexual abuse material as well as to lay down and disseminate contents to raise awareness and prevent child sexual

abuse.

Or. en

Amendment 476
Annalisa Tardino

Proposal for a regulation
Recital 69 b (new)

Text proposed by the Commission

Amendment

(69b) To make the best use of survivors knowledge, the EU Centre shall consult with victims organisations and helplines to set up and improve victims support mechanisms as well as to analyse and explore new forms of online sexual abuses.

Or. en

Amendment 477
Lucia Ďuriš Nicholsonová, Fabienne Keller, Yana Toom

Proposal for a regulation
Recital 70

Text proposed by the Commission

Amendment

(70) Longstanding Union support for both INHOPE and its member hotlines recognises that hotlines are in the frontline in the fight against online child sexual abuse. The EU Centre should leverage the network of hotlines and encourage that they work together effectively with the Coordinating Authorities, providers of relevant information society services and law enforcement authorities of the Member States. The hotlines' expertise and experience is an invaluable source of information on the early identification of common threats and solutions, as well as on regional and national differences across

(70) Longstanding Union support for both INHOPE and its member hotlines recognises that hotlines are in the frontline in the fight against online child sexual abuse. ***This role played by hotlines should be reinforced and they should continue to facilitate this fight. Each Member State should ensure that at least one official hotline is operating in its territory.*** The EU Centre should leverage the network of hotlines and encourage that they work together effectively with the Coordinating Authorities, providers of relevant information society services and law enforcement authorities of the Member

the Union.

States. The hotlines' expertise and experience is an invaluable source of information on the early identification of common threats and solutions, as well as on regional and national differences across the Union. *Anonymous public reporting is crucial to countering child sexual abuse and hotlines have created a worldwide network and procedures for the child sexual abuse identification and removal. Member States should ensure that the public has the possibility to anonymously report child sexual abuse material and child sexual exploitation activities to hotlines specialised in combatting online child sexual abuse material and shall safeguard the role of such hotlines in anonymous public reporting. The promotion of hotlines by the EU Centre and the Coordinating Authorities through the educational systems of Member States in order to educate youth and reach potential victims is of great importance. The experience of hotlines and other non-governmental organizations involved in reporting or proactive searching of child sexual abuse material and expertise should help the EU Centre and Coordinating Authorities to design appropriate prevention techniques and awareness campaigns and keeping the databases of indicators up to date.*

Or. en

Amendment 478
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 71

Text proposed by the Commission

Amendment

(71) Considering Europol's mandate and its experience in identifying competent national authorities in unclear situation and its database of criminal

deleted

intelligence which can contribute to identifying links to investigations in other Member States, the EU Centre should cooperate closely with it, especially in order to ensure the swift identification of competent national law enforcement authorities in cases where that is not clear or where more than one Member State may be affected.

Or. en

Amendment 479
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 72

Text proposed by the Commission

Amendment

(72) Considering the need for the EU Centre to cooperate intensively with Europol, the EU Centre's headquarters should be located alongside Europol's, which is located in The Hague, the Netherlands. The highly sensitive nature of the reports shared with Europol by the EU Centre and the technical requirements, such as on secure data connections, both benefit from a shared location between the EU Centre and Europol. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol, notably those regarding human resources management, information technology (IT), including cybersecurity, the building and communications. Sharing such support services is more cost-efficient and ensure a more professional service than duplicating them by creating them anew.

deleted

Or. en

Amendment 480

Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 72

Text proposed by the Commission

Amendment

(72) Considering the need for the EU Centre to cooperate intensively with Europol, the EU Centre's headquarters should be located alongside Europol's, which is located in The Hague, the Netherlands. The highly sensitive nature of the reports shared with Europol by the EU Centre and the technical requirements, such as on secure data connections, both benefit from a shared location between the EU Centre and Europol. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol, notably those regarding human resources management, information technology (IT), including cybersecurity, the building and communications. Sharing such support services is more cost-efficient and ensure a more professional service than duplicating them by creating them anew.

deleted

Or. en

Amendment 481
Fabienne Keller, Nathalie Loiseau

Proposal for a regulation
Recital 72

Text proposed by the Commission

Amendment

(72) Considering the need for the EU Centre to cooperate intensively with Europol, the EU Centre's headquarters should be located alongside Europol's, which is located in The Hague, the Netherlands. The highly sensitive nature of the reports shared with Europol by the

(72) The EU Centre's headquarters should be *decided on the basis of objective criterias* between the *Parliament and the Council in an ordinary legislative procedure*.

EU Centre and the technical requirements, such as on secure data connections, both benefit from a shared location between the EU Centre and Europol. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol, notably those regarding human resources management, information technology (IT), including cybersecurity, the building and communications. Sharing such support services is more cost-efficient and ensure a more professional service than duplicating them by creating them anew.

Or. en

Amendment 482
Annalisa Tardino

Proposal for a regulation
Recital 72

Text proposed by the Commission

(72) ***Considering the need for the EU Centre to cooperate intensively with Europol, the EU Centre's headquarters should be located alongside Europol's, which is located in The Hague, the Netherlands. The highly sensitive nature of the reports shared with Europol by the EU Centre and the technical requirements, such as on secure data connections, both benefit from a shared location between the EU Centre and Europol. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol, notably those regarding human resources management, information technology (IT), including cybersecurity, the building and communications. Sharing such support services is more cost-efficient and ensure a more professional service than duplicating them by creating them anew.***

Amendment

(72) ***The EU Centre should conclude a headquarters agreement with the host Member State in a timely manner before it begins operations. In light of the case-law of the Court of Justice, the choice of the location of the seat should be made in accordance with the ordinary legislative procedure and should comply with the criteria laid down in this Regulation.***

Amendment 483
Annalisa Tardino

Proposal for a regulation
Recital 72 a (new)

Text proposed by the Commission

Amendment

(72a) Considering that a relevant number of child sexual material online present in the internal market is produced in Third countries, the EU Centre should cooperate with competent services in relevant international forum to prevent child sexual abuses at global level.

Or. en

Amendment 484
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 74

Text proposed by the Commission

Amendment

(74) In view of the need for technical expertise in order to perform its tasks, ***in particular the task of providing a list of technologies that can be used for detection***, the EU Centre should have a Technology Committee composed of experts with advisory function. ***The Technology Committee may, in particular, provide expertise to support the work of the EU Centre, within the scope of its mandate, with respect to matters related to detection of online child sexual abuse, to support the EU Centre in contributing to a high level of technical standards and safeguards in detection technology.***

(74) In view of the need for technical expertise in order to perform its tasks, the EU Centre should have a Technology Committee composed of experts with advisory function.

Or. en

Amendment 485

Fabienne Keller, Nathalie Loiseau

Proposal for a regulation

Recital 74

Text proposed by the Commission

(74) In view of the need for technical expertise in order to perform its tasks, in particular the task of providing a list of technologies that can be used for detection, the EU Centre should have a Technology Committee composed of experts with advisory function. The Technology Committee may, in particular, provide expertise to support the work of the EU Centre, within the scope of its mandate, with respect to matters related to detection of online child sexual abuse, to support the EU Centre in contributing to a high level of technical standards and safeguards in detection technology.

Amendment

(74) In view of the need for technical expertise in order to perform its tasks, in particular the task of providing a list of technologies that can be used for detection, the EU Centre should have a Technology Committee composed of experts with advisory function. The Technology Committee may, in particular, provide expertise to support the work of the EU Centre, within the scope of its mandate, with respect to matters related to detection of online child sexual abuse, to support the EU Centre in contributing to a high level of technical standards and safeguards in detection technology, **and the evolution of those technologies and developing new ones.**

Or. en

Amendment 486

Lucia Ďuriš Nicholsonová, Fabienne Keller

Proposal for a regulation

Recital 74

Text proposed by the Commission

(74) In view of the need for technical expertise in order to perform its tasks, in particular the task of providing a list of technologies that can be used for detection, the EU Centre should have a Technology Committee composed of experts with advisory function. The Technology Committee may, in particular, provide expertise to support the work of the EU

Amendment

(74) In view of the need for technical expertise in order to perform its tasks, in particular the task of providing a list of technologies that can be used for detection, the EU Centre should have a Technology Committee composed of experts with advisory function. The Technology Committee may, in particular, provide expertise to support the work of the EU

Centre, within the scope of its mandate, with respect to matters related to detection of online child sexual abuse, to support the EU Centre in contributing to a high level of technical standards and safeguards in detection technology.

Centre, within the scope of its mandate, with respect to matters related to detection **and prevention** of online child sexual abuse, to support the EU Centre in contributing to a high level of technical standards and safeguards in detection technology.

Or. en

Amendment 487

Hilde Vautmans, Olivier Chastel, Fabienne Keller, Maite Pagazaurtundúa, Lucia Ďuriš Nicholsonová, Nathalie Loiseau

Proposal for a regulation

Recital 74 a (new)

Text proposed by the Commission

Amendment

(74a) The Technology Committee could therefore establish a certification for technologies which could be used by online service providers to detect child sexual abuse material on their request.

Or. en

Amendment 488

Cornelia Ernst, Clare Daly

Proposal for a regulation

Recital 75

Text proposed by the Commission

Amendment

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on anonymised

deleted

gathering of non-personal data and to publish annual reports on their activities under this Regulation. The Coordinating Authorities should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

Or. en

Amendment 489
Rob Rooken

Proposal for a regulation
Recital 75

Text proposed by the Commission

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on anonymised gathering of non-personal data and to publish annual reports on their activities under this Regulation. The Coordinating Authorities should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

Amendment

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available ***number independent*** interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on anonymised gathering of non-personal data and to publish annual reports on their activities under this Regulation. The Coordinating Authorities should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

Or. en

Amendment 490
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 75

Text proposed by the Commission

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on *anonymised* gathering of non-personal data and to publish annual reports on their activities under this Regulation. The Coordinating Authorities should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

Amendment

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on gathering of non-personal data and to publish annual reports on their activities under this Regulation. The Coordinating Authorities should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

Or. en

Justification

Non-personal data cannot be anonymised, nor can gathering of non-personal data.

Amendment 491
Cornelia Ernst, Clare Daly

Proposal for a regulation
Recital 76

Text proposed by the Commission

(76) In the interest of good governance and drawing on the statistics and information gathered and transparency reporting mechanisms provided for in this Regulation, the Commission should carry out an evaluation of this Regulation within *five* years of the date of its entry into force,

Amendment

(76) In the interest of good governance and drawing on the statistics and information gathered and transparency reporting mechanisms provided for in this Regulation, the Commission should carry out an evaluation of this Regulation within *two* years of the date of its entry into force,

and every *five* years thereafter.

and every *two* years thereafter.

Or. en

Amendment 492

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 77

Text proposed by the Commission

(77) The evaluation should be based on the criteria of efficiency, necessity, effectiveness, proportionality, relevance, coherence and Union added value. It should assess the functioning of the different operational and technical measures provided for by this Regulation, ***including the effectiveness of measures to enhance the detection, reporting and removal of online child sexual abuse, the effectiveness of safeguard mechanisms as well as the impacts on potentially affected fundamental rights, the freedom to conduct a business, the right to private life and the protection of personal data. The Commission should also assess the impact on potentially affected interests of third parties.***

Amendment

(77) The evaluation should be based on the criteria of efficiency, necessity, effectiveness, proportionality, relevance, coherence and Union added value. It should assess the functioning of the different operational and technical measures provided for by this Regulation.

Or. en

Justification

All elements of the Regulation should be assessed.

Amendment 493

Rob Rooken

Proposal for a regulation

Recital 78

Text proposed by the Commission

(78) Regulation (EU) 2021/1232 of the European Parliament and of the Council⁴⁵ provides for a temporary solution in respect of the use of technologies by certain providers of publicly available interpersonal communications services for the purpose of combating online child sexual abuse, pending the preparation and adoption of a long-term legal framework. This Regulation provides that long-term legal framework. Regulation (EU) 2021/1232 should therefore be repealed.

⁴⁵ Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (OJ L 274, 30.7.2021, p. 41).

Amendment

(78) Regulation (EU) 2021/1232 of the European Parliament and of the Council⁴⁵ provides for a temporary solution in respect of the use of technologies by certain providers of publicly available **number independent** interpersonal communications services for the purpose of combating online child sexual abuse, pending the preparation and adoption of a long-term legal framework. This Regulation provides that long-term legal framework. Regulation (EU) 2021/1232 should therefore be repealed.

⁴⁵ Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (OJ L 274, 30.7.2021, p. 41).

Or. en

Amendment 494

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 1

Text proposed by the Commission

This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse **in** the internal market.

Amendment

This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse, **in order to contribute to the proper functioning of** the internal market **and to create a safe, predictable and trusted online environment that facilitates**

innovation and in which fundamental rights enshrined in the Charter are effectively protected.

Or. en

Justification

in line with DSA

Amendment 495

Paul Tang, Alex Agius Saliba

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 1

Text proposed by the Commission

This Regulation lays down uniform rules to address the *misuse* of relevant information society services for online child sexual abuse in the internal market.

Amendment

This Regulation lays down uniform rules to address the *use* of relevant information society services for online child sexual abuse in *order to contribute to the proper functioning of* the internal market *and to create a safe, predictable and trusted online environment where fundamental rights enshrined in the Charter are effectively protected.*

Or. en

Amendment 496

Moritz Körner, Sophia in 't Veld, Yana Toom, Morten Petersen, Abir Al-Sahlani, Michal Šimečka, Jan-Christoph Oetjen, Svenja Hahn, Karen Melchior

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 1

Text proposed by the Commission

This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse in the internal market.

Amendment

This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse in the internal market *by persons suspected of being involved in child sexual abuse and persons disqualified*

from exercising activities involving children.

Or. en

Amendment 497
Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 1

Text proposed by the Commission

This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse in the internal market.

Amendment

This Regulation lays down uniform rules to ***prevent and*** address the misuse of relevant information society services for online child sexual abuse in the internal market.

Or. en

Amendment 498
Jadwiga Wiśniewska

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 1

Text proposed by the Commission

This Regulation lays down uniform rules to address the ***misuse*** of relevant information society services for online child sexual abuse in the internal market.

Amendment

This Regulation lays down uniform rules to ***prevent and*** address the ***use*** of relevant information society services for online child sexual abuse in the internal market.

Or. en

Amendment 499
Charlie Weimers, Cristian Terheş, Rob Rooken

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point b

Text proposed by the Commission

Amendment

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse *where there is reasonable cause to suspect such illegal behaviour*;

Or. en

Amendment 500

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point b

Text proposed by the Commission

Amendment

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

(b) obligations on providers of hosting services and providers of *publicly available number-independent* interpersonal communication services to detect and report online child sexual abuse *in specific cases*;

Or. en

Amendment 501

Cornelia Ernst, Clare Daly

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point b

Text proposed by the Commission

Amendment

(b) obligations on providers of hosting services and providers of interpersonal *communication* services to *detect and* report online child sexual abuse;

(b) obligations on providers of hosting services and providers of *number independent communications* services to report online child sexual abuse *and to cooperate with the EU Centre*;

Or. en

Amendment 502

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point b

Text proposed by the Commission

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

Amendment

(b) obligations on providers of hosting services and providers of ***number-independent*** interpersonal communication services to detect and report online child sexual abuse;

Or. en

Amendment 503

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Birgit Sippel, Petar Vitanov

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point b

Text proposed by the Commission

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

Amendment

(b) obligations on providers of hosting services and providers of ***number-independent*** interpersonal communication services to detect and report online child sexual abuse;

Or. en

Amendment 504

Rob Rooker

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point b

Text proposed by the Commission

(b) obligations on providers of hosting services and providers of interpersonal communication services to ***detect and***

Amendment

(b) obligations on providers of hosting services and providers of interpersonal communication services to ***cooperate with***

report online child sexual abuse;

the EU Centre;

Or. en

Amendment 505
Rob Rooken

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point c

Text proposed by the Commission

Amendment

(c) obligations on providers of hosting services to remove or disable access to child sexual abuse material on their services;

(c) obligations on providers of hosting services to remove or disable access to **known** child sexual abuse material on their services;

Or. en

Justification

In the case of hosting providers or providers of internet access services, the legal obligation to remove or disable (access to) content must only contain known and confirmed child sexual abuse material, in order to avoid false positives, and protect people's fundamental rights and private sphere.

Amendment 506
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point c

Text proposed by the Commission

Amendment

(c) obligations on providers of hosting services to remove **or disable access to** child sexual abuse material on their services;

(c) obligations on providers of hosting services to remove child sexual abuse material on their services;

Or. en

Amendment 507

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point c

Text proposed by the Commission

Amendment

(c) obligations on providers of hosting services to remove **or disable access to** child sexual abuse material on their services;

(c) obligations on providers of hosting services to remove child sexual abuse material on their services;

Or. en

Amendment 508

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point c

Text proposed by the Commission

Amendment

(c) obligations on providers of hosting services to remove **or disable access to** child sexual abuse material on their services;

(c) obligations on providers of hosting services to remove child sexual abuse material on their services;

Or. en

Amendment 509

Cornelia Ernst, Clare Daly

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point c

Text proposed by the Commission

Amendment

(c) obligations on providers of hosting services to remove **or disable access to** child sexual abuse material on their services;

(c) obligations on providers of hosting services to remove **known** child sexual abuse material on their services;

Amendment 510
Cornelia Ernst, Clare Daly

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point d

Text proposed by the Commission

Amendment

(d) obligations on providers of internet access services to disable access to child sexual abuse material; *deleted*

Amendment 511
Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point d

Text proposed by the Commission

Amendment

(d) obligations on providers of internet access services to disable access to child sexual abuse material; *deleted*

Amendment 512
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point d

Text proposed by the Commission

Amendment

(d) obligations on providers of internet access services to disable access to child sexual abuse material; *deleted*

Amendment 513

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point d

Text proposed by the Commission

Amendment

(d) *obligations on providers of internet access services to disable access to child sexual abuse material;* *deleted*

Or. en

Amendment 514

Rob Rooker

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point d

Text proposed by the Commission

Amendment

(d) obligations on providers of internet access services to disable access to child sexual abuse material;

(d) obligations on providers of internet access services to disable access to **known** child sexual abuse material;

Or. en

Amendment 515

Hilde Vautmans, Fabienne Keller, Olivier Chastel, Maite Pagazaurtundúa, Abir Al-Sahlani, Lucia Ďuriš Nicholsonová, Nathalie Loiseau

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point d a (new)

Text proposed by the Commission

Amendment

(da) obligations on providers of online search engines and any other artificial intelligence systems to delist or disable specific items of child sexual abuse, or both;

Or. en

Amendment 516

Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point d a (new)

Text proposed by the Commission

Amendment

(da) obligations on providers of online search engines to delist websites which were determined to host child sexual abuse material;

Or. en

Amendment 517

Paul Tang, Alex Agius Saliba

Proposal for a regulation

Article 1 – paragraph 1 – subparagraph 2 – point e

Text proposed by the Commission

Amendment

(e) rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member States, *the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre')* and cooperation and transparency.

(e) rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member States;

Or. en

Justification

Moved the EU Centre to a separate point

Amendment 518
Paul Tang, Alex Agius Saliba

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point e a (new)

Text proposed by the Commission

Amendment

(ea) rules on the designation, functioning, cooperation, transparency and powers of the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre');

Or. en

Amendment 519
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 1 – paragraph 1 – subparagraph 2 – point e a (new)

Text proposed by the Commission

Amendment

(ea) Obligations on providers of online games.

Or. en

Amendment 520
Patrick Breyer
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 1 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. This Regulation shall only apply to services normally provided for remuneration.

Justification

In line with the legal basis of internal market, the definitions of hosting services (Art. 3 (g) and (a) of Regulation (EU) 2022/2065, Article 1(1), point (b), of Directive (EU) 2015/1535) and communications services (Article 2 (5) of Directive (EU) 2018/1972) are limited to services normally provided for remuneration. For reasons of legal certainty and foreseeability this should be explicitly stated in this Regulation.

Amendment 521

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 1 – paragraph 2 b (new)

Text proposed by the Commission

Amendment

2b. This Regulation does not apply to audio communications.

Amendment 522

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 1 – paragraph 3 – point b

Text proposed by the Commission

Amendment

(b) Directive 2000/31/EC and Regulation (EU) .../... ***[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]***;

(b) Directive 2000/31/EC and Regulation (EU) **2022/2065** (Digital Services Act);

Amendment 523

Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Article 1 – paragraph 3 – point b a (new)

Text proposed by the Commission

Amendment

(ba) Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online;

Or. en

Amendment 524
Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation
Article 1 – paragraph 3 – point d

Text proposed by the Commission

Amendment

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725, **and, subject to paragraph 4 of this Article**, Directive 2002/58/EC.

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725 **and** Directive 2002/58/EC.

Or. en

Amendment 525
Cornelia Ernst, Clare Daly

Proposal for a regulation
Article 1 – paragraph 3 – point d

Text proposed by the Commission

Amendment

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725, **and, subject to paragraph 4 of this Article**, Directive 2002/58/EC.

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725 **and** Directive 2002/58/EC.

Or. en

Amendment 526

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 3 – point d

Text proposed by the Commission

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725, and, ***subject to paragraph 4 of this Article***, Directive 2002/58/EC.

Amendment

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725, and Directive 2002/58/EC.

Or. en

Amendment 527

Jadwiga Wiśniewska

Proposal for a regulation

Article 1 – paragraph 3 – point d a (new)

Text proposed by the Commission

Amendment

(da) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)"

Or. en

Amendment 528

Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation

Article 1 – paragraph 3 – point d a (new)

Text proposed by the Commission

Amendment

(da) Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive);

Or. en

Amendment 529

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 3 – point d a (new)

Text proposed by the Commission

Amendment

(da) Regulation (EU) .../... [laying down harmonised rules on artificial intelligence (Artificial Intelligence Act);

Or. en

Amendment 530

Cornelia Ernst, Clare Daly

Proposal for a regulation

Article 1 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. Nothing in this Regulation shall be interpreted as prohibiting, restricting or undermining, including de-facto, the provision or use of encrypted and end-to-end encrypted services. Providers shall not in particular be prohibited or discouraged from offering end-to-end encrypted services, and the provision of such services shall not be made, including de-facto, difficult, financially unsustainable, or impossible.

Amendment 531
Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Article 1 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. This regulation shall not have the effect of modifying the obligation to respect the rights, freedom and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to the right to private life and family life and to freedom of expression and information;

Or. en

Amendment 532
Paul Tang, Alex Agius Saliba, Birgit Sippel, Theresa Bielowski, Tiemo Wölken, Marina Kaljurand

Proposal for a regulation
Article 1 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. This Regulation shall not prohibit, weaken or undermine end-to-end encryption, prohibit providers of information society services from providing their services applying end-to-end encryption, or be interpreted in that way.

Or. en

Amendment 533
Cornelia Ernst, Clare Daly

Proposal for a regulation
Article 1 – paragraph 3 b (new)

Text proposed by the Commission

Amendment

3b. This Regulation shall be without prejudice to the rules on professional secrecy under national law, such as rules on the protection of professional communications, between doctors and their patients, between journalists and their sources, or between lawyers and their clients, in particular since the confidentiality of communications between lawyers and their clients is key to ensuring the effective exercise of the rights of the defence as an essential part of the right to a fair trial.

Or. en

Amendment 534

Paul Tang, Alex Agius Saliba, Birgit Sippel, Theresa Bielowski, Tiemo Wölken, Marina Kaljurand, Patrick Breyer

Proposal for a regulation
Article 1 – paragraph 3 b (new)

Text proposed by the Commission

Amendment

3b. This Regulation shall not undermine the prohibition of general monitoring under Union law or introduce general data retention obligations, or be interpreted in that way.

Or. en

Amendment 535

Vincenzo Sofo, Jadwiga Wiśniewska

Proposal for a regulation
Article 1 – paragraph 3 b (new)

Text proposed by the Commission

Amendment

3b. *Nothing in this Regulation shall be interpreted as prohibiting or weakening end-to-end encryption.*

Or. en

Amendment 536
Cornelia Ernst, Clare Daly

Proposal for a regulation
Article 1 – paragraph 3 c (new)

Text proposed by the Commission

Amendment

3c. *This Regulation does not provide for a lawful basis for the processing of personal data for the sole purpose of detecting child sexual abuse on a voluntary basis.*

Or. en

Amendment 537
Cornelia Ernst, Clare Daly

Proposal for a regulation
Article 1 – paragraph 4

Text proposed by the Commission

Amendment

4. *This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC insofar as necessary for the execution of the detection orders issued in accordance with Section 2 of Chapter 1 of this Regulation.*

deleted

Or. en

Amendment 538

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 4

Text proposed by the Commission

4. This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC insofar as necessary for the execution of the detection **orders** issued in accordance with Section 2 of Chapter 1 of this Regulation.

Amendment

4. This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC **with the sole objective of enabling providers of number-independent interpersonal communications services, without prejudice to Regulation (EU) 2016/679, to use specific technologies for the processing of personal data to the extent strictly necessary to detect and report child sexual abuse material and remove child sexual abuse material on their services** insofar as necessary for the execution of the detection **warrants** issued in accordance with Section 2 of Chapter 1 of this Regulation.

Or. en

Amendment 539

Paul Tang, Alex Agius Saliba, Birgit Sippel

Proposal for a regulation

Article 1 – paragraph 4

Text proposed by the Commission

4. This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC **insofar as necessary for the execution of the** detection **orders** issued in accordance with Section 2 of Chapter 1 of this Regulation.

Amendment

4. This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC **with the sole objective of enabling a provider of hosting services, a provider of number-independent interpersonal communications services or a provider of an artificial intelligence**

system to use specific technologies for the processing of personal data to the extent strictly necessary to detect and report online child sexual abuse and remove child sexual abuse material on their services, following a detection warrant issued in accordance with Section 2 of Chapter 1 of this Regulation.

Or. en

Amendment 540

Charlie Weimers, Cristian Terheş, Rob Rooker

Proposal for a regulation

Article 1 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. To ensure fundamental rights laid down in the European Union's, the Council of Europe's and the United Nation's human rights charters, core fundamentals of our democratic society and the rule of law - citizens' right to privacy and private correspondence must be upheld. Therefore, detection orders can only be issued towards persons suspected of criminal activity. There shall be no general monitoring of ordinary law-abiding citizens and users of interpersonal communication services private messages.

Or. en

Justification

Human rights offline shall also apply online, as stated in the United Nations Human Rights Council resolution A/HRC/RES/20/8.

Amendment 541

René Repasi, Tiemo Wölken

on behalf of the S&D Group

Petar Vitanov

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

Birgit Sippel

**Proposal for a regulation
Article 1 – paragraph 4 a (new)**

Text proposed by the Commission

Amendment

4a. This Regulation does not apply to audio communications.

Or. en

**Amendment 542
Paul Tang, Alex Agius Saliba, Birgit Sippel**

**Proposal for a regulation
Article 1 – paragraph 4 a (new)**

Text proposed by the Commission

Amendment

4a. This Regulation does not apply to audio communications.

Or. en

**Amendment 543
René Repasi, Tiemo Wölken
on behalf of the S&D Group
Petar Vitanov
on behalf of the Committee on Civil Liberties, Justice and Home Affairs
Birgit Sippel**

**Proposal for a regulation
Article 1 – paragraph 4 b (new)**

Text proposed by the Commission

Amendment

4b. This Regulation does not apply to text communications.

Or. en

Amendment 544

Patrick Breyer

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 2 – paragraph 1 – point a

Text proposed by the Commission

(a) ‘hosting service’ means ***an information society*** service as defined in Article 2, point ***(f)***, third indent, of Regulation (EU) .../... ***[on a Single Market For Digital Services*** (Digital Services Act) ***and amending Directive 2000/31/EC***];

Amendment

(a) ‘hosting service’ means ***a hosting*** service as defined in Article 3, point ***(g)***, third indent, of Regulation (EU)***2022/2065*** (Digital Services Act);

Or. en

Justification

correct reference 3, point g, third indent