



TRANSPARENCY REPORT 2025

e-Enfance as a Trusted Flagger under article 22 of the Digital Services Act

This first transparency report of e-Enfance/3018 covers the period from 1 January to 31 December 2025. It presents the activity of 3018 as France's first trusted flagger under the Digital Services Act and highlights the operational challenges faced in the reporting and removal of harmful online content involving minors.

*Reporting period
1 January - 31 December 2025*

A national helpline and a trusted flagger for child online protection

Who is e-Enfance/3018 ?

Founded in 2005 and recognized as a public interest organization since 2010, the e-Enfance/3018 association protects minors and young adults from harassment and digital risks by combining prevention, support, listening, and intervention. It operates under the national number 3018, handling 124,500 requests in 2025 thanks to its multidisciplinary teams (psychologists, lawyers, child protection experts).

Designated as the first trusted flagger by the French National Regulation Authority (Arcom) on November 8, 2024, 3018, e-Enfance's operational system transmits documented reports to platforms in accordance with the DSA (EU Regulation 2022/2065), while guaranteeing its independence and the traceability of its interventions.

Today, **e-Enfance / 3018 is the trusted flagger submitting the highest volume of notices to social media platforms in Europe.** It therefore acts as a major entry point for harmful content affecting minors.

Online content often reveals broader situations of risk : vulnerability, coercion, family violence, sexual violence, isolation, school dropout, or psychological distress.

Our missions :

- **Prevention** : Raising awareness among young people, parents and professionals.
- **Helpline 3018** : Assessing situations, supporting victims and reporting to platforms.
- **Advocacy** : Contributing to public policies and safer digital practices.
- **Observatory** : Analysing digital violence and identifying emerging trends.

Key figures - 2025

- **124,500 requests received by 3018**
- **44,028 cases handled**
- **214,003 downloads of the 3018 app since launch**
- **7 days a week helpline availability**

3018: The French National Helpline and a central pillar of the trusted flagger system

A unique organisation in France thanks to its specialised teams, structured approach and ability to act in often complex situations.

The situations handled reflect the diversity of digital violence to which minors are exposed: harassment, cyberbullying, non-consensual sharing of intimate images, sexual extortion (sextortion), blackmail, identity theft, doxxing, digital mobbing and exposure to harmful content.

A multidisciplinary team

3018 relies on specialised teams trained in digital violence and harassment mechanisms, including psychologists, lawyers, social workers and former members of the national police force. the helpline is open 7 days a week, 9 a.m. to 11 p.m. (anonymous, confidential, free of charge), simultaneous translation into 180 languages, accessibility for deaf and hard-of-hearing people.

Operational data

- **44,028** contacts handled
- **85%** of victims were involved in harmful situations
- **60 to 75 minutes** average processing time for each report
- **180 languages** available through simultaneous translation

Online reporting is not only a technical process. It requires listening, legal analysis, contextual understanding and human support.

3018 is a Helpline that can be reached by phone, email, webchat via the website, chat via the 3018 mobile app, and through a direct action within two VLOPs in their “Harassment Reporting” pathways (a direct call button on Instagram and a link to 3018 on TikTok). This diversity of contact channels ensures proximity, responsiveness and safety, while providing teams with reliable information for analysing cases. In 2025, 25.88% of cases required multiple contacts.

Key figures - trusted flagger activity

Framework :

- 4,150 requests for the removal of online accounts or content (3,326 concerning minor victims / 824 concerning victims aged 18 to 25)
- As part of its trusted flagger status: 1,946 requests concerned content published on online platforms.
- Outside Article 22 but within the scope of the DSA: 5 requests concerned hosting service providers.
- Outside the scope of the DSA: 2,199 requests concerned content shared through private interpersonal communication services and were handled according to their internal procedures.

16.4% of the reports received concern "fisha accounts". In France, "fisha" accounts derived from the French slang of "afficher" (to display) and refers to social media accounts created and used to share images, videos, or private information of girls and women without their consent, with the intent to humiliate and publicly expose them.

Scope of action

- **Very Large Online Platforms (VLOPS)**
- **Very Large Online Search Engines (VLOSE)**
- **Online platforms** : Content published on services falling within the trusted flagger framework.
- **Hosting service providers** : Reports handled within the broader scope of the DSA.
- **Private interpersonal communication services** : Situations handled according to providers' internal procedures, outside Article 22.

On Snapchat (43%), YouTube (34.5%) and Facebook (30%), more than one in two reported pieces of content remain online. On X, nearly three out of four reported pieces of content are not removed.

Reporting mechanisms remain highly fragmented across platforms

The report identifies significant differences in the way trusted flagger notices can be submitted and followed up.

Field experience reveals six distinct levels of compliance with the reporting obligations set out in Articles 16 and 22 of the DSA:

Level 1 : *Dedicated notification portal (Meta, TikTok, Discord and eBay)* : trusted flagger status is clearly identified, notices are tracked, and follow-up or appeal procedures are managed efficiently.

Level 2 : *Dedicated email or form for trusted flaggers (Snapchat, Google, Telegram, WhatsApp)* : priority treatment is guaranteed in principle, but the processing status of submitted notices is not visible.

Level 3 : *Article 11 contact point, also used by trusted flaggers (Shein)*: no guarantee of priority treatment and no tracking of processing status.

Level 4 : *General form or email with explicit mention of trusted flaggers (X, Pinterest, Roblox, Reddit)* : priority processing guaranteed in principle, but no tracking of processing status.

Level 5 : *General form or email with no mention of trusted flaggers (Temu, Bigo live, CapCut, Twitch, Yubo and others)*: no guarantee of priority treatment; trusted flagger notices risk being processed as ordinary user reports, in potential non-compliance with Article 22.

Level 6 : *Absent or non-functional reporting mechanism (Doxbin, KikFriender, Leakimedia, Rencontre Ados)*: users and trusted flaggers are unable to report illegal content, which may amount to non-compliance with Articles 16 and 22 of the DSA.

Cooperation between trusted flaggers and platforms

Since its designation as a trusted reporting organisation, the e-Enfance/3018 Association has been contacted by certain platforms informing it that dedicated reporting channels have been set up (Dailymotion, eBay). These measures, which include specialised contact points, reduced processing times and direct communication with moderation teams, enable reports to be processed more quickly and efficiently and facilitate the interruption of online violence. Regular exchanges with platforms also help to improve reporting tools and strengthen the protection of minors (Google, YouTube, Snapchat, Tiktok). These best practices show that structured cooperation between platforms and trusted flaggers is an essential lever for reducing processing times and limiting minors' exposure to online violence.

Uneven platform responses and follow-up

The report highlights significant differences in platform responses, both in terms of response times and the quality of decisions.

Several providers acknowledge receipt of notices and process them quickly, sometimes within 48 hours. These practices contribute to the rapid removal of illegal content and to limiting minors' exposure to online violence.

However, the report also identifies areas requiring vigilance. Some responses remain unclear, partial or insufficiently documented. In some cases, platforms indicate that action has been taken without specifying the measure implemented, making it difficult to provide clear information to victims.

Some platforms also rely on alternative measures such as geoblocking, temporary suspension or warnings. These measures may be insufficient when they do not ensure the complete and permanent removal of harmful content.

Examples from VLOPs and VLOSEs

TikTok

- 1,021 notices submitted
- 845 removals
- 98,8% response rate ;
83% removal rate

Instagram

- 326 notices submitted
- 181 removals
- 55.5% removal rate

Snapchat

- 227 notices submitted
- 97 removals
- 43% removal rate

X

- 65 notices submitted
- 15 removals
- 100% response rate ;
23% removal rate

YouTube

- 52 notices submitted
- 18 removals
- 96% response rate ;
34.5% removal rate

BLOGGER (Google)

- 63 notices submitted
- 34 removals
- 95% response rate ; 70%
removal rate

Discord

- 44 notices submitted
- 20 removals
- 95.5% response rate ;
45.5% removal rate

Roblox

- 7 notices submitted
- 0 removals
- 71.5% response rate ; 0%
removal rate

Telegram

- 36 notices submitted
- 29 removals
- 97% response rate ;
80.6% removal rate

Our experience shows that the effectiveness of trusted flagger notices cannot be assessed only through response rates: what matters for victims is whether harmful content is actually removed, clearly documented and followed up.

A wide range of digital violence affecting minors

The situations handled by 3018 reflect the diversity and seriousness of online violence affecting minors.

Reports involve harassment, cyberbullying, non-consensual sharing of intimate images, sexual extortion, blackmail, identity theft, doxxing, digital mobbing and exposure to harmful content. Among these, 'fisha' accounts (social media accounts created to publicly expose girls and women by sharing their private images or personal information without consent, with the explicit intent to humiliate), represent one of the most reported content categories, with 321 notices submitted in 2025, 301 of which concerned minor victims.

These cases often require legal qualification, contextual analysis and coordination between several forms of support. They also show that the protection of minors online cannot be reduced to content removal alone. This is further confirmed by a striking shift in who is reaching out for help: in 2025, the average age of people contacting 3018 dropped from 20 to 15 years old, while the proportion of victims involved in harmful situations rose from 65% to 85%, a clear signal that younger children are now directly exposed to the most severe forms of online violence.

Main harms identified

- **Cyberbullying and harassment** : Repeated violence, humiliation and coordinated attacks.
- **Non-consensual sharing of intimate images**: Dissemination of private images without consent.
- **Sexual extortion and blackmail** : Pressure, threats and coercion targeting minors.
- **Doxxing and identity theft** : Exposure of personal data and impersonation.
- **Exposure to harmful content** : Pornographic, violent, hateful or otherwise harmful content.

The diversity of harms requires a protection response combining victim support, reporting, legal expertise and follow-up.

The 2025 Vigilancemeter: turning field experience into regulatory insight

The Vigilometer is an annual tool that synthesises the findings emerging from the Prevention Unit, the 3018 Helpline, the Observatory and e-Enfance/3018's advocacy work. It is designed to raise awareness among regulators and platforms regarding good practices, areas requiring particular vigilance and potential violations of the Digital Services Act, while encouraging the development of digital services that offer stronger protection for minors.

Good practices identified

Good practices include implementation of a dedicated notification portal for trusted flaggers, an active moderation by the platform prior to the intervention of the trusted flagger and the organisation of collaborative meetings with the e-Enfance/3018 Association.

Points of vigilance

A key point of vigilance concerns the lack of harmonisation across platforms, both in terms of the evidence required to submit a report and the legal assessment needed to qualify harmful content.

Depending on the platform, and sometimes even within the same platform, the required supporting elements may vary significantly: the author's pseudonym or ID, screenshots, URL links, or a combination of several elements. This fragmentation makes the reporting process more complex and increases the risk of delays or errors. It is also reinforced by the heterogeneity of platforms' terms and conditions of use, which requires legal advisors to carry out detailed and platform-specific assessments. In addition, some platforms provide unclear or insufficiently documented responses.

For certain offences, platforms such as Snapchat, Roblox and Yubo may indicate that appropriate measures have been taken without specifying what those measures are. In such cases, the 3018 Helpline cannot provide clear information to victims, who remain uncertain about the outcome of their report.

Another point of vigilance concerns the use of geoblocking measures in France, which may restrict access to content nationally without ensuring its effective removal from the platform.

DSA violations

The report also identifies potential DSA compliance issues.

First, some platforms, including Cam4Joy, KikFriender, Leakimedia, SecretNote.me and ImgBB, do not provide a clear contact point or an effective mechanism enabling users, including trusted flaggers, to report illegal content or behaviour. The absence of such a mechanism may constitute non-compliance with the DSA, as the 3018 Helpline has encountered significant difficulties, and in some cases failed entirely, to contact the relevant hosting provider. Second, the report highlights the absence of age-verification mechanisms on platforms such as Stripchat, WatchPeopleDie, Chatiw.com and Skibbel.com, despite the fact that they provide access to content that is dangerous or inappropriate for minors.

By failing to implement reasonable measures to prevent minors from accessing pornographic or gory content, these platforms expose young users to serious risks and may fall short of the obligations imposed by the DSA.

The recommendations of the Association e-Enfance/3018 in light of the findings from its first year as a trusted flagger

The findings presented in the transparency report underline the central role of the Association e-Enfance/3018 within the DSA ecosystem and the need to strengthen regulatory practices.

In this regard, the Association e-Enfance/3018 puts forward a set of recommendations aimed at improving the effectiveness of the reporting mechanism in order to enhance operational responses and coordination of actions to protect minors with online platforms.

- **Strengthening the technical architecture for reporting content involving minors**

Require online platforms to provide a priority notification channel dedicated to trusted flaggers.

In accordance with Article 22 of Regulation (UE) 2022/2065 on digital services, providers of online platforms must ensure that notifications submitted by trusted flaggers are processed with priority and without undue delay.

In practice, the effective implementation of this priority requires that platforms be able to clearly identify notifications submitted by trusted flaggers and ensure that they are subject to specific processing. Accordingly, each platform falling within the scope of Article 22 of the DSA must establish a sure priority notification channel accessible to trusted flaggers and separate from the channel made available to the general public. This channel must allow for the qualified submission of reports, identification of the notifier's status, tracking the processing status, and the management of follow-ups.

Platforms must also provide a secondary notification channel to ensure continuity of processing in the event of unavailability or malfunction of the main channel. The absence of an operational notification mechanism, or the provision of non-functional systems, cannot be regarded as compliant with the obligations laid down in articles 16 and 22 of the DSA.

→ *Establishing a harmonised European nomenclature for reporting content involving minors*

The operational experience of the 3018 helpline highlights significant fragmentation in reporting mechanisms across platforms, both in their structure and in their methods of access. This heterogeneity leads to a substantial increase in processing times and places a disproportionate burden on the resources required to submit notifications.

We recommend the adoption of a **harmonised nomenclature at the European level applicable to reports concerning content involving minors**. This framework should include common fields allowing, in particular, the identification of the reported content or account, the legal qualification of the facts, the legal basis invoked, the emergency nature of the situation, the age of the victim where known, as well as contextual elements necessary to assess the level of risk.

This nomenclature should also harmonise the requirements relating to the evidence requested by platforms. Analysis of reporting procedures reveals significant divergences in the supporting materials required, including within the same service. This variability lengthens processing times and increases the risk of misclassification.

The definition of a **common set of information and evidentiary elements** would help provide legal certainty to notification procedures and reduce the technical obstacles encountered by victims and by the actors responsible for reporting such content.

Regulating notification processing times and requiring a justified response from platforms

Observations from the 3018 helpline reveal significant disparities in the processing times for notifications sent to platforms. While some are handled within a few hours, others take several weeks or receive no response at all.

In this context, it is necessary to clarify the requirements applicable to platforms regarding the processing of notifications submitted by trusted flaggers. In particular, platforms should be required to :

- provide immediate acknowledgement of receipt for submitted notifications;
- indicate the maximum processing time applicable to the report;
- provide an explicit and justified response, including in cases where no action is taken.

• Improving the quality of moderation of content involving minors

→ Promoting a standard of qualified human moderation adapted to risks affecting minors

Online platforms should ensure that the handling of reports relating to content involving minors relies on human moderation with skills appropriate for analyzing such situations.

For this purpose, platform providers should establish moderation teams with human resources proportionate to the size of the service, the number of active users, and the risks identified in the operation of the platform.

Moderators responsible for handling these reports must be trained to understand the legal, social, linguistic and cultural issues that may help clarify the context in which the reported content or behaviors occur, particularly when they involve minors.

Such an approach would help ensure a more accurate assessment of submitted reports, especially when they include contextual elements related to the vulnerability of victims or the repetition of harmful acts.

→ Integrating the contextualization of reports into moderation mechanisms

In accordance with Article 16 of Regulation (EU) 2022/2065 on digital services, providers of online platforms must make available mechanisms allowing the notification of the presence of illegal content through sufficiently substantiated notices.

In this context, platforms should take into account the contextual elements accompanying notifications submitted by trusted flaggers specialized in the protection of minors, including the age of the victim, identified vulnerabilities, the history of the acts, or the accumulation of harms, and should incorporate these contextual elements into the analysis of reports in order to identify and prioritize the handling of situations revealing repeated violence or particular vulnerability involving minors.

This consideration should also lead platforms to establish internal escalation mechanisms when notifications submitted by a trusted flagger reveal a serious risk to the integrity of a minor, particularly in cases of sexual exploitation, blackmail, or psychological endangerment.

→ *Ensuring the effective removal of illegal content involving minors rather than relying on geoblocking*

Some platforms respond to reports submitted by 3018 by making content inaccessible from the territory of certain Member States while keeping it accessible in other jurisdictions. Such a practice of territorial restriction of access does not put an end to the dissemination of the content on the service and does not ensure effective protection of victims.

Where the reported content is manifestly illegal or harmful, particularly in cases involving the non-consensual dissemination of sexual content, cyberbullying, or serious violations of a minor's dignity, territorial limitation of access cannot constitute a sufficient response in light of the due diligence obligations set out in Regulation (EU) 2022/2065.

We call on platforms to proceed with the **effective removal of such content across the service**, rather than limiting themselves to geoblocking measures restricted to national or European territory.

Strengthening the specific obligations applicable to Very Large Online Platforms (VLOPs)

→ *Integrating a referral mechanism to 3018, a trusted flagger specialized in the protection of minors, into VLOPs' reporting pathways*

In accordance with Article 16 of Regulation (EU) 2022/2065, online platforms must provide accessible and effective notification mechanisms enabling users to report the presence of illegal content.

The guidelines relating to Article 28 of the DSA also recall that these mechanisms must be designed in a clear and understandable way for minors so that they can easily identify the protection and assistance services available to them.

In this context, Very Large Online Platforms should integrate, within their reporting pathways, a referral mechanism to **3018**, a trusted flagger specialized in addressing online violence involving minors. Already implemented by some major platforms, the integration of a dedicated button **directly linking to 3018** helps improve the visibility of reporting mechanisms for minors and ensures rapid and appropriate support for reported situations, in addition to the platform's own moderation mechanisms.

→ *Providing dedicated application programming interfaces (APIs) for the processing of reports relating to minors*

For Very Large Online Platforms, the notification mechanism provided for in Article 16 of Regulation (EU) 2022/2065 should be complemented by the provision of application programming interfaces (APIs) relating to content involving minors.

These interfaces would in particular enable the secure and automated transmission of the elements constituting the report, as well as the monitoring of their processing, in addition to the priority notification channel provided for trusted flaggers under Article 22 of the Regulation.

Such technical interconnection would help reduce the time required for the transmission and processing of reports and ensure the effective prioritization of notifications concerning situations involving minors.

→ *Enabling the suspension of accounts used to initiate an offense targeting a minor*

Analyses conducted by 3018 show that many offenses targeting minors are initiated on online platforms falling within the scope of Regulation (EU) 2022/2065, before being pursued on interpersonal communication services.

These situations notably involve acts of sexual solicitation of minors, sexual extortion, manipulation, or coercive control, in which the initial contact occurs on an online platform before the exchanges are transferred to an interpersonal communication service.

In such configurations, the analysis carried out by the 3018 teams makes it possible, through legal qualification and the contextualization of reports, to identify the platform account that was used to initiate the situation and to establish a factual link between this account and the subsequent commission of the offense on a third-party service.

However, in practice, some platforms refuse to take measures against the account that was used to initiate the offense on the grounds that the offense subsequently continued on a service outside their own infrastructure.

It is essential that the notice-and-action mechanisms provided for in Article 16 of Regulation (EU) 2022/2065 allow for the consideration of contextual elements establishing that the use of a platform account served to initiate or facilitate an offense targeting a minor.

Where such elements are transmitted by a trusted flagger with the meaning of Article 22 of Regulation (EU) 2022/2065 and make it possible to identify with sufficient certainty the account that was used to initiate the situation, providers of online platforms should be required to take appropriate measures against that account, including its suspension or removal, even where the commission of the offense subsequently continued on an interpersonal communication service.

It is essential that the notice-and-action mechanisms provided for in Article 16 of Regulation (EU) 2022/2065 allow for the consideration of contextual elements demonstrating that the use of a platform account served to initiate or facilitate an offense targeting a minor.

Where such elements are transmitted by a trusted flagger within the meaning of Article 22 of Regulation (EU) 2022/2065 and make it possible to identify, with sufficient certainty, the account used to initiate the situation, providers of online platforms should be required to take appropriate measures against that account, including its suspension or removal, even where the offense subsequently continued on an interpersonal communication service.

→ *Integrating data from specialized reports into the analysis of systemic risks*

Providers of Very Large Online Platforms and Very Large Online Search Engines are required, under Article 34 of Regulation (EU) 2022/2065, to conduct regular assessments of the systemic risks arising from the functioning and use of their services, particularly with regard to negative effects on the safety, security or health of minors.

In practice, these assessments rely mainly on internal data derived from moderation systems or from the analysis of service usage. However, this approach has certain limitations, insofar as some dynamics that place minors at risk can only be identified through a contextualized analysis of situations reported by victims, their relatives, or the professionals supporting them.

We call for the risk assessments provided for under Article 34 to also incorporate data derived from qualified reports submitted by trusted flaggers within the meaning of Article 22 of the Regulation. These reports are based on a human and contextualized analysis of situations and make it possible to identify types of risks that the platform's automated tools do not always detect.

Such integration would make it possible to more precisely identify features or digital environments that may expose minors to particular risks, particularly recommendation systems, user-matching mechanisms, or certain community spaces, and to adapt the mitigation measures provided for under Article 35 of the Regulation accordingly.

- **Strengthening the supervision and evaluation of the DSA**

→ *Strengthening oversight of the effectiveness of notice-and-action mechanisms (Articles 16 and 22)*

Compliance with the obligations set out in Regulation (EU) 2022/2065 concerning notice-and-action mechanisms cannot be assessed solely on the basis of the formal existence of a reporting system. Article 16 of the DSA requires providers of online platforms to make available mechanisms enabling the notification of illegal content, while Article 22 provides for the priority treatment of notifications submitted by trusted flaggers.

Observations from the 3018 helpline, however, show that certain notification systems, although formally in place, do not in practice allow for the effective processing of reports. This situation may arise in particular from the inaccessibility of notification mechanisms, technical malfunctions, or the absence of effective processing of submitted notifications.

We call on the authorities responsible for supervising Regulation (EU) 2022/2065, the national Digital Services Coordinators, as well as the European Commission for very large online platforms, to include in their compliance oversight an assessment of the actual effectiveness of these mechanisms.

Such an assessment should, in particular, verify that the notification systems provided for under Articles 16 and 22 of the DSA effectively enable the submission and processing of reports and are not limited to purely formal compliance.

→ *Integrating the quality and contextualisation of reports into DSA supervision*

It would be appropriate for the regulator and the European Commission to incorporate, into their assessment of platform compliance, indicators relating to the qualitative consideration of reports submitted by trusted flaggers.

This assessment should not be limited to the volume of reports received or to observed processing times, but should also include an analysis of how platforms take into account the contextual elements accompanying these notifications, particularly when they concern complex situations involving minors.

This perspective would allow for a more precise evaluation of the effectiveness of the due diligence obligations provided for under Regulation (EU) 2022/2065, especially when reports submitted by 37

trusted flaggers contain information relating to the vulnerability of victims, the repetition of the acts, or the accumulation of harms.

→ *Better addressing the displacement of risks across digital services*

The European Commission could assess the opportunity to extend the analysis of systemic risks to digital environments that serve as vectors for contact or the displacement of interactions involving minors, in particular online games and interpersonal communication services.

- **Ensuring the clarity and sustainability of the trusted flagger system**

→ *Clarifying the area of expertise of trusted flaggers to improve the routing of reports and the coordination of child protection*

The trusted flagger mechanism established in Article 22 of Regulation (EU) 2022/2065 is based on the recognition of entities with a specific area of expertise in identifying and reporting illegal content. In certain fields, the handling of reports requires coordination with other protection mechanisms, including judicial, educational, social or medical-psychological systems.

In this context, it seems relevant for the competent authorities responsible for implementing the Regulation to take into account the specialization of trusted flaggers and their area of expertise when organizing the system provided for in Article 22. Such an approach could help strengthen coordination between platforms and public actors, while improving the clarity of the system for users, notably by making it easier to identify the entities best suited to handle reports in specific domains.

→ *Creating a European mechanism for sustainable funding of trusted flaggers specialized in the protection of fundamental rights*

The effectiveness of the reporting system provided for in Article 22 of Regulation (EU) 2022/2065 relies largely on the action of trusted flaggers responsible for identifying, qualifying and notifying platforms of allegedly illegal content within their area of expertise. In certain fields, notably the protection of minors, these entities play a central role in detecting risks and transmitting essential information to platforms and competent authorities.

However, unlike the supervisory system established by the Regulation, no specific financial mechanism is provided to support the activity of trusted flaggers. This contrasts with the mechanism established in Article 43 of the DSA, which provides for an annual fee payable by Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to cover the costs incurred by the European Commission in carrying out its supervisory tasks.

To ensure the effectiveness of the missions provided for in Article 22, a European mechanism for sustainable funding by contributions from VLOPs and VLOSEs, following a logic similar to that set out in Article 43 of the Regulation.

The allocation of funding should be based on objective criteria reflecting the actual activity of trusted flaggers within the system established by the DSA, notably :

The volume of qualified reports submitted to platforms specifically under the priority handling mechanism provided for in Article 22 ;

- The operational capacity of the entity, assessed in particular with regard to the human resources deployed for the analysis, qualification and follow-up of reports ;
- The legal and technical quality of notifications submitted under Article 16 of the Regulation ;
- The technical investments required to ensure the traceability and reliability of reports ;
- The interdisciplinary expertise mobilized for the contextualized qualification of situations, particularly when they involve minors.

Such a mechanism would ensure the sustainability of trusted flaggers contributing to the effective protection of fundamental rights in the European digital environment, while guaranteeing that resources are allocated in line with the area of expertise for which these entities were designated under Article 22 of Regulation (EU) 2022/2065.

[Read the detailed transparency report](#)

e- enfance 30 18

Ensemble, agissons pour
un monde numérique
responsable

Association Reconnue d'Utilité Publique

