Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
zu 20(23)131

17.05.2023

The Cologne Prosecutor-General's Office
The Cybercrime Centre and Contact Point
of North Rhine-Westphalia – ZAC NRW

Statement for the public hearing held by the German Bundestag's Committee on Digital Affairs on the subject of "chat control" on 1 March 2023

I. Preliminary remarks

The Cybercrime Centre and Contact Point of North Rhine-Westphalia (ZAC NRW) is a hybrid institution attached to the Cologne Public Prosecution Office and the Cologne Prosecutor-General's Office. Under section 3 of the General Administrative Act issued by the Justice Ministry of 15 March 2016 as amended on 17 December 2021 (4100 - III. 274, Cybercrime Centre General Administrative Act (ZAC-AV)), the part of the Cybercrime Centre attached to the Public Prosecution Office conducts major investigations into cybercrime offences in the narrower sense and – in the case of certain special digital criminal phenomena – cybercrime in the broader sense in North Rhine-Westphalia. These special criminal phenomena include online criminal offences against the sexual self-determination of children and young people; specifically, this refers to overarching proceedings in the form of investigations of persons unknown, in which large quantities of digital evidence is analysed with the aim of identifying accused persons, as well as to investigations across the whole of North Rhine-Westphalia into cases resulting from the reporting obligation established by section 3a (2) no. 3 b) of the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*) and from reports provided by the US National Center for Missing and Exploited Children (NCMEC) and similar organisations. Apart from this field of crime, investigations into attacks on critical infrastructure, agencies, public institutions and enterprises make up a particularly large part of the Cybercrime Centre's work, and in this context the Cybercrime Centre deals with a wide range of information security issues.

The part of the Cybercrime Centre attached to the Cologne Prosecutor-General's Office is the cybercrime contact point for North Rhine-Westphalia. Its tasks include, under section 4.1 of the Cybercrime Centre General Administrative Act (ZAC-AV), responsibility for fundamental questions in the field of cybercrime that are unrelated to a specific investigation, and, under section 4.3 of the General Administrative Act, responsibility for research with the aim of developing and updating practical methods and techniques for law enforcement. To this end, the Cybercrime Centre collaborates with national and international partners from the research community and business. Key research projects are currently being undertaken in the field of the use of artificial intelligence to automatically assess child and youth pornographic[1] visual and video content. In its capacity as a contact point, the Cybercrime Centre also deals with questions about the use and effects of cryptography in the context of investigations.

The Cybercrime Centre and Contact Point of North Rhine-Westphalia is thus essentially an operational law enforcement institution whose research and development work is focused on supporting investigations and criminal proceedings, and on enabling modern technical developments to be used by law enforcement agencies in practice. In this statement, the European Commission's "chat control" proposals are therefore assessed primarily from the perspective of public prosecution office and general law enforcement practice. The

[1] This statement mainly uses the legal terminology used in Division 13 of the Special Part of the Criminal Code (*Strafgesetzbuch*).

perspectives of prevention, improved compliance and other effects on societal, political and technical issues are discussed only where they intersect with law enforcement, given my organisation's area of expertise.

II. Individual questions

With that said, I would like to turn now to the individual questions; given the limited time available at the hearing, I have kept my responses very brief.

1) The European Commission's proposal for a CSA Regulation, also known as the "chat control" proposal, has been the subject of a great deal of discussion since its publication in May 2022. Please explain the technical, legal, fundamental-rights, data-protection, social and/or societal implications of the proposal.

The European Commission's proposal for a Regulation laying down rules to prevent and combat child sexual abuse (the draft CSAM Regulation), which is intended to replace the Interim Regulation currently in force, Regulation (EU) 2021/1232 of 14 July 2021, has implications – insofar as it aims to harmonise the internal market through uniform EU rules to prevent and combat child sexual abuse – for the work of the national law enforcement agencies which deal with the criminal phenomenon of child abuse in the digital sphere. To date, the major internet companies (such as Facebook/Meta, Microsoft, Google/Alphabet) have voluntarily carried out scanning activities to identify child abuse material in unencrypted messages and emails, as well as hosted files and posted content. Now these activities are to be made mandatory, with uniform obligations being established for "all providers of hosting or interpersonal communication services offering such services in the EU's digital single market" (hereinafter: service providers) – i.e. for hosting service providers, interpersonal communication services (messaging services and email), app stores and access providers, among others. The obligations will depend on the type of service, and are intended to prevent hosting and communication services from being used in future for the dissemination of child sexual abuse material or the solicitation of children, known as "grooming".

The following five elements of the proposal are particularly important for law enforcement practice, although the data-protection, social, societal and/or technical aspects are only examined here from the specific perspective of law enforcement agencies.

1. Preventive risk assessment and mitigation obligation

In future, service providers are to be required to perform a risk assessment to determine whether and to what extent their services can be misused for the dissemination of child sexual abuse material or for the solicitation of children, and to adopt measures to mitigate these risks. If the introduction of age verification is also considered in this context, this is likely to make any anonymous use of communication services impossible in practice, as it seems likely that minors can only be effectively excluded from using the services through a functionality enabling personal identification; simply asking users to confirm their age would not be effective. Regarding the implications for the open-source ecosystem, please see my answer to question 7.

2. Targeted detection obligations on the basis of detection orders

If the assessment carried out by a national coordinating authority to be designated by the Member States concludes that, despite any risk mitigation measures taken, there remains a significant risk of the service being used in the context of child abuse (see Article 7 of the draft CSAM Regulation), the coordinating authorities to be established at national level will be able to ask a court or an independent administrative authority to issue detection orders for a limited period which require the detection of a certain type of content in a specific service. These orders will require service providers to detect known or unknown child sexual abuse

material or the solicitation of children, in line with and using indicators provided by an EU Centre, which is still to be established. The result is that service providers are forced, when ordered, to monitor the content of their services. If service providers become the addressees of such a detection order, they are required to use technologies which meet certain requirements for the implementation of a detection order; these requirements are set out in Article 10 (3) of the draft CSAM Regulation. The provider can choose whether to use their own software for this purpose, or software developed by the EU Centre on Child Sexual Abuse (see Article 10 (2) and Articles 40 to 42 of the draft CSAM Regulation). On the one hand, the technologies used must contribute effectively to the detection of the dissemination of known or new child sexual abuse material or the solicitation of children; on the other hand, they must have a reliably low error rate when it comes to the extraction of relevant information, in order to minimise the extent to which other information is affected. The technologies must also reflect the state of the art and minimise the interference in fundamental rights associated with their use. Against this backdrop, and considering the amount of data to be examined, the communication services and intermediaries will effectively only be able to meet their obligation via a fully automated, largely AI-based assessment of the communication content – and so ultimately the proposal only appears to be technology-neutral. If, in view of the requirements clearly defined in the proposal and the expected amount of data and content, the monitoring mechanisms can realistically only be implemented in the form of full knowledge and automated scanning of a service's entire content, this represents an interference in European (and national) fundamental rights, with the intensity and form of this interference depending on the specifics of how this is implemented and on the type of service and content concerned. Please see my response to question 3.

Regarding the technologies used, a distinction is likely to have to be made: providers of communication services which are unencrypted or which only encrypt data in transit (e.g. emails, the messaging services of social networks such as Facebook, Instagram, Twitter) can be expected, given the substance of the Regulation, to use server-side algorithms to ensure automated detection of child abuse material and grooming messages. The situation is different for providers of end-to-end encrypted communication (such as WhatsApp, Threema, Signal). In this case, it is technically impossible to examine the communication content, because it is encrypted. While the proposal for a Regulation leaves open how, from a technical perspective, the providers of such communication services are to meet their obligation in future, encrypted providers are not excluded from the Regulation's scope and thus are equally obliged to examine content as provided for by the Regulation. They will be required to check the content prior to encryption, i.e. to incorporate a mechanism in the app or service itself which checks the message before it is sent – and thus before it is encrypted. In the case of end-to-end encrypted content, this ultimately means that – assuming that the encryption is not to be removed entirely or technologically weakened – the checks will have to take place on users' devices, which is known as client-side scanning. Communication services and intermediaries will be expected to examine and assess communication content directly on the device – before it is sent – and to extract it, if suspicions exist. The implementation of detection orders thus has significant implications for information security, as it ultimately introduces an intentional vulnerability in encryption technology, and the risks and the potential for misuse are evident.

The envisaged implementation of detection orders can be expected, given the high error rates of the technologies used, to result in billions of pieces of communication content being monitored; certainly, millions of conversations (including private conversations) and private image and video files – a significant proportion of which will fall within the sphere of absolute privacy – of large numbers of EU citizens will be flagged and will have to be examined and

checked by a large number of reviewers, even if the proposal provides for automated checks in the first instance and for human review only at a subsequent stage at the EU Centre.

3. Reporting obligations and removal of illicit material

Service providers are to be required to report content deemed to be relevant to a new EU Centre, and to remove child sexual abuse material without delay. If removal is not possible, the service providers are to be required to block access to images and videos (see Articles 16 to 18 of the draft CSAM Regulation). If service providers do not comply with their obligation to remove or block access to material, the national authorities will have the power to issue a removal order. Regarding the effectiveness of access-blocking mechanisms, please see my answer to question 15.

4. Monitoring mechanisms and redress

To minimise the risk of false positives and erroneous reports, reports of suspected child sexual abuse produced in this way are to be checked by the EU Centre before they are forwarded. In addition, "various measures are [to be] taken to ensure effective redress for both providers and users" (see the provisions in Articles 9, 15 and 18 of the draft CSAM Regulation). For example, providers of hosting services and providers of interpersonal communications services that have received a detection order, as well as users affected by the measures taken to execute it, are to have a right to effective redress, which includes the right to challenge the detection order before the courts of the Member State of the competent judicial authority or independent administrative authority that issued the detection order (see Article 9 of the draft CSAM Regulation). Given the complexity of exercising this right for individual users – especially in the European legal context – it remains questionable whether individual redress can be an adequate corrective to any misuse of detection orders. It thus falls to providers to guarantee their users' rights, a role which they are hardly in a position to fulfil properly, in view of their primarily commercial interests. The introduction of a strong, independent oversight mechanism is highly advisable in this context.

5. Establishment of an EU Centre

The proposal provides for the creation of a European Centre to prevent and counter child sexual abuse (the EU Centre), which will serve as an expertise and coordination hub, in particular. For example, the EU Centre's tasks are to include providing indicators for the detection of child sexual abuse and creating the necessary databases, receiving reports from service providers, and checking (erroneous) reports. In addition, the EU Centre will assist the national authorities with carrying out their envisaged tasks, and support victims in removing content related to them. Furthermore, content is to be forwarded – provided that the suspicion that it constitutes abuse material is confirmed – to Europol or national law enforcement agencies (see Article 48 of the draft CSAM Regulation).

2) The Commission's proposal provides for the issuance of detection orders requiring providers of communications services or devices to covertly access information if it is suspected that abuse material is being shared via these services or devices or that grooming is taking place on them. In your view, what services and devices are potentially affected by this and to what extent, and what effects will this have on their users?

Detection orders do not require the service to in fact be used on a significant scale for child abuse. Rather, for such an order to be issued, it is sufficient for there to be a significant risk – irrespective of the scale – of the service being used for this purpose (see Article 7 (4) of the draft CSAM Regulation), meaning that in future all digital communication services and devices are likely to be covered by the provisions of the draft Regulation. It seems clear,

including from the breadth of the definition of providers (see Article 2 of the draft CSAM Regulation), that there is no intention to limit the scope to specific services; in particular, the proposal does not include any size or usage thresholds.

3) Why, in your opinion, is the Commission's proposal fit for purpose or not fit for purpose when it comes to protecting children effectively from (sexual) abuse and the dissemination of abuse material, and where do you believe concrete action is needed?

Criminal law consists, to a special degree, of the application of the principle of proportionality. Law enforcement at any price is not a viable alternative – irrespective of the field of crime in question – under German and European constitutional law. From the specific perspective of a law enforcement agency, the Commission's proposal must therefore, in line with the traditional three-part test of proportionality, be suitable, necessary and proportionate, in the narrower sense, to achieve the aim of combating child sexual abuse offences (see recital 1). (Technical) suitability must always be viewed in the context of a concrete assessment of proportionality. The proportionality of detection orders, in particular, must be considered, given that they touch on law enforcement practice, but to a lesser extent the proportionality of the EU Centre and of the reporting obligation for illicit content must also be examined.

Taking each of these in turn:

1. Detection orders

The detection order, which is the core element of the Commission's proposals that touches on law enforcement practice, appears not to be entirely necessary to achieve the aim of improved and effective action to combat online child abuse. There are also concerns – some of them serious – regarding its suitability.

a) No concerns exist regarding the fundamental legitimacy of the aim of combating very serious criminal offences in the field of online child sexual abuse (see recital 13), or the legitimacy of the envisaged means, namely public regulation of certain online actions.

b) The means envisaged in the Commission's proposal, namely a detection order, is also likely to be suitable, i.e. at least beneficial in relation to the intended aim. The proposed measures can be expected both to increase the number of online child sexual abuse offences that are detected and to promote the identification of individual suspects. When looking at suitability, another factor to consider is the possibility of a shift to technologies and providers which thwart detection orders by ensuring that users alone control the encryption keys or the encryption process, or which simply withdraw from EU jurisdiction. Such shifts can be expected, but are likely to be limited in scale relative to the total volume of communications. In any case, based on the practical experience of the Cybercrime Centre and Contact Point of North Rhine-Westphalia, the proposed measure should not be regarded as manifestly unsuitable.

c) However, significant and ultimately serious concerns already exist regarding the necessity of at least part of the measures associated with the detection order, especially insofar as they are directed against end-to-end encrypted communication. A measure is necessary to achieve an aim if a less restrictive measure is not possible, or if a less restrictive measure does not appear equally suitable to achieve the aim.

The Commission's proposal provides for a mechanism, in the form of the detection order established by Article 7 et seqq. of the draft CSAM Regulation, in which the coordinating authorities to be established at national level can ask a court or an independent administrative authority to issue orders – for a limited period and for the detection of a specific type of content in a specific service – making it mandatory to detect known or unknown child sexual abuse material or grooming. This means that service providers are

required, when ordered, to monitor the content of their services. The detection order is based on a risk-based approach, according to Article 7 (4) of the draft CSAM Regulation.

The Commission's proposal seems to assume that an intelligence and information deficit exists for law enforcement, as a result of which law enforcement agencies are unable to take action on the necessary scale to effectively combat these offences. Admittedly, current law enforcement practice (see 3 below) depends to a significant extent on reports from US companies to the US National Center for Missing and Exploited Children (NCMEC). Insofar as technical instruments such as server-side scanning of unencrypted user content (or user content that is only encrypted in transit) and effective reporting mechanisms for end users are necessary for a functional European equivalent offering full legal certainty, it is not clear that similarly effective but less invasive instruments exist. In this context, it must also be taken into account that, in the case of server-side access to unencrypted user content, users knowingly give access to their data to third parties – the providers – and thus this data leaves the core area of the private sphere.

Even if, remarkably, the Commission's proposal largely avoids the term "end-to-end encryption", it can be assumed, given the specific design of Article 10 of the draft CSAM Regulation, that the Commission has (primarily) focused on upstream or downstream access to encrypted communications through device-side access to the content as a means of addressing concerns that law enforcement agencies are unable to access this content.

End-to-end encrypted communications, as a matter of principle, represent a particular obstacle for law enforcement agencies, as they – if properly implemented – effectively restrict access to the information required in investigations, in the sense of cleartext communication data. Nonetheless, end-to-end encryption of offenders' communications in the field of crime being discussed here, that of online child abuse, proves to be a serious obstacle to investigations only in a very small number of cases. It is impossible to say whether this is primarily due to effective investigative methods, a lack of technical knowledge on the part of the offenders, or other technical causes, such as the bandwidth limits of encrypted communication methods for multimedia files. It is also important to consider the breadth of the intelligence that can be obtained from a combination of findings from server-side surveillance, from investigations themselves, and from reports from third parties (see above).

The Commission's focus is significantly out of touch with the reality of law enforcement practice, at least with regard to end-to-end encrypted communication. The main obstacle is not that offences are not being detected due to encryption, or the existence of offence-related platforms or offence-specific dissemination methods.

Instead, there are structural shortcomings in terms of action, caused by law enforcement agencies being understaffed and under-resourced in technical terms. These problems are visible at almost levels of the criminal investigation process. The analysis of digital evidence takes too long – sometimes several years – and this holds back the progress of investigations. Not enough specialised police investigation teams are available, and this results in current intelligence simply being processed consecutively. High-quality technical and specialised investigative work, including to neutralise and parallelise encryption in individual cases, is so constrained by the limited resources that the quantity and quality of investigative work under criminal procedure law inevitably falls far short of what would be possible if adequate resources were available. It is impossible to make full use of all appropriate options within the legally permitted framework established by the Code of Criminal Procedure (*Strafprozessordnung*) in every case due to the shortage of resources. It is clear from the contacts which the Cybercrime Centre and Contact Point of North Rhine-Westphalia has at national and international level that this state of affairs is not limited to the Cybercrime Centre's area of responsibility; it is a fundamental problem.

By comparison with client-side scanning, in any case, strengthening law enforcement practice represents an at least equally suitable but much less invasive measure to achieve the envisaged improvement of law enforcement in relation to online child abuse offences in the wider sense. In the course of dealing with a major child abuse case known as “Bergisch Gladbach”, the Cybercrime Centre and Contact Point of North Rhine-Westphalia, which was tasked with handling this case, reorganised itself from 2020 onwards. Its staffing levels were significantly increased, and it set up a specialised Task Force to Combat Child Abuse and the Dissemination of Child Pornography in Digital Media. Across the whole of North Rhine-Westphalia, in cooperation with North Rhine-Westphalia’s Criminal Police Office, all reports received from foreign partners, such as NCMEC, are now viewed and initially processed by the Cybercrime Centre. In addition, special departments have been set up for investigations into platforms and infrastructures that facilitate and promote online child abuse. As a result of these measures – as well as other factors, such as an increase in the number of reports – we have managed to more than double the number of Cybercrime Centre investigations of identified perpetrators across the entire field of Division 13 of the Special Part of the Criminal Code in 2022 by comparison with 2021, and have even achieved a six-fold increase in the number of investigations of unidentified perpetrators. It can be assumed that the underlying criminal phenomenon has not fundamentally changed; however, because the law enforcement agencies were better positioned, they have been able to detect a much bigger proportion of the “dark field” of unreported crime. Adopting this approach systematically at European level as well would, in view of the interests of the criminal justice system, represent a contribution that is at least as effective as an unlimited detection order, but without the need to abandon the key principle that a public prosecution office (only) acts if there are sufficient factual indications that a specific offence has been committed (an “initial suspicion”; see section 152 (2) of the Code of Criminal Procedure) by introducing a merely risk-based instrument, in the form of the detection order. Concrete, effective law enforcement which is always based on a reasonable suspicion of wrongdoing is likely, by comparison with a risk-based general intervention, to be a significantly less restrictive, but (at least) equally suitable means of better combating online child abuse, including in end-to-end encrypted communication infrastructures.

d) While well-founded arguments can be made that detection orders are necessary with regard to server-side scanning of unencrypted user content, such a measure would also have to be deemed to be proportionate in the narrower sense. For this to be the case, the relevant interference in fundamental rights would have to not be disproportionate to the objective being pursued. The German Bundestag’s Research Services rightly point out in their study of 7 October 2022 (WD 10 - 3000 - 026/22; to avoid duplication, please see the study itself regarding this point) that it seems improbable “that general surveillance of individual communication would be found to be consistent with (European) fundamental rights. […] Based on the specified issues and problems, the current draft Regulation provides for disproportionate interferences in respect of the relevant fundamental rights laid down in the Charter of Fundamental Rights” (see section 6 of the study).

In this context, the study focuses mainly on the weakness of AI-based solutions and highlights how prone to error they are. However, for server-side scanning of unencrypted user content, it would probably be advisable to use hashes, also known as “digital fingerprints”, which offer a precise detection method. As a matter of principle, this method can only detect known material which has been classified as abuse material, as hash-based methods, unlike AI solutions, focus on the recognition of known material, whereas artificial intelligence is also meant to detect previously unknown abuse material. Hash-based solutions avoid the weaknesses of AI solutions, at the price of not detecting unknown, newly generated content. This kind of entirely automated, comparative and non-evaluative process ought to significantly minimise the degree of interference in fundamental rights, with the

result that this level of interference is deemed to be suitable. The detection delta regarding unknown abuse material, which law enforcement agencies regard as inevitable, can be effectively addressed by strengthening law enforcement agencies as discussed in c) above, as in the vast majority of typical cases, suspects also – at least complementarily – disseminate and possess known child abuse material. Effective investigative work by law enforcement agencies on the basis of intelligence generated from server-side scanning using hash values is likely to prove to be a sufficiently effective measure to enable law enforcement agencies, in the course of their investigations, to also track down people who produce and/or disseminate unknown abuse material, without it being necessary to resort to the much more invasive method of an evaluative use of AI and breaking encryption. If the EU Centre succeeds in establishing an effective, unbureaucratic and time-efficient way of maintaining hash databases, the hash filter quality can also be expected to continuously improve as a result of investigations conducted on the basis of reports, etc.

Finally, from the perspective of a cybercrime centre, end-to-end encryption's paramount importance in terms of information security should, as a precaution, be emphasised in the context of the criteria to be considered when examining suitability. End-to-end encryption is the only effective means of protecting the confidentiality of digital communication. It is the most important digital safeguard not just for individuals, but also for companies, public agencies, and not least for law enforcement – including for specially protected professional groups, such as defence lawyers. From a technical perspective, encryption is either effective or compromised. Encryption which is weakened or structurally undermined by an instrument such as a detection order is, in practice, not encryption at all. The Commission's proposals would introduce a fundamental vulnerability and are, in relation to encrypted communication content, disproportionate from this perspective as well.

2. EU Centre

From the perspective of law enforcement practice, enhanced European cooperation between investigating authorities is welcome. An EU Centre can play a key part in this. This applies, initially, to ensuring a standardised European approach to intelligence. A greater operational focus in the Centre's tasks, set out in Article 43 of the proposal, would also be desirable. This is not to overlook the fact that various aspects of the Commission's proposal call for cooperation between the EU Centre and Europol. Nonetheless, European law enforcement practice requires a much greater degree of European coordination and initiative.

A greater focus on the judicial side of law enforcement, through a suitable form of involvement – for example via Eurojust – would also be positive, as it can be assumed that effective European law enforcement impetus can only be generated by a law enforcement alliance that is not limited to police cooperation.

Furthermore, it could be advisable to give the EU Centre, alone or in cooperation with Europol, concrete responsibility for European coordination of law enforcement in the case of online child abuse offences. The current mechanisms are proving to be inadequate in practice. For example, when it comes to transnationally relevant platforms on which illicit material is shared and crimes are initiated or communicated, not enough has been done to ensure that the law enforcement efforts of the European Member States are properly coordinated and that the relevant intelligence is shared in a simple and accessible process. Multinational joint investigation teams are only set up on a long-term basis for specific investigations, not for specific fields of crime, even though it could be beneficial to establish "standing" multinational investigation teams for certain particularly relevant types of crime, such as online child abuse. Although the EU Centre is to play more of an advisory, supportive and administrative-executive role under the Commission's proposal, the legislative initiative is inadequate from the perspective of law enforcement practice –

including with regard to the European legislative competences – without concrete links to law enforcement.

3. Reporting obligation

Providers which have detected or otherwise become aware of online child sexual abuse material are to be required to report it to the EU Centre. From a law enforcement perspective, such a reporting obligation is to be welcomed unreservedly. Currently, NCMEC reports are of paramount importance and make up the vast majority of intelligence which leads to investigations being launched. Setting up a European institution ought to significantly expand the pool of reports and provide a sound legal basis for the reporting providers beyond the scope of application of US legislation.

4) How great is the risk, in your view, of innocent members of the public coming under suspicion due to false positives produced by automated detection, and what would the impact of such false positives be for both the suspects and the investigating authorities?

Since 2017, the Cybercrime Centre and Contact Point of North Rhine-Westphalia has been researching, together with science and business partners, the possibilities of using artificial intelligence to automatically detect child and youth pornographic content in digital evidence. The lessons learned from this experience should also be applicable to automated detection in the case of online communications. The main challenge when using automated detection is carefully balancing the detection focus. The tool used should miss as little illicit content as possible (false negatives) while wrongly identifying as little legally unobjectionable content as possible (false positives). These two objectives clash with each other. If the focus is minimising false positives, there is a danger that significant quantities of illicit communications would not be detected. Conversely, maximising the detection rate of genuinely illicit content would inevitably result in a higher false positive rate. The risk of innocent members of the public coming under suspicion due to false positives produced by automated detection is therefore not a static calculation. The AI tool developed by the Cybercrime Centre and its partners, AIRA (AI-enabled rapid assessment), currently detects more than 90% of the relevant illicit content with a false positive rate in the mid to low single-digit percentage range. If these figures are applied to the detection order process and the large amounts of content which would be processed, there is a significant risk that innocent members of the public would be subject to official investigations. This is particularly true with regard to the AI-based miscategorisation of cases where the visual material itself is detected accurately, but the situation under criminal law is misjudged. To give an example, this includes cases where children below the age of criminal responsibility have posted material themselves, or communications between young people in consensual contexts (see section 184c (4) of the Criminal Code).

False positives ultimately represent a misallocation of resources for the investigating authorities, as in fact no initial suspicion exists that an offence has been committed. The draft CSAM Regulation provides for reports to first be filtered by the EU Centre, and so it can be assumed that the Centre will bear the burden of providing these additional resources. However, from a law enforcement perspective, there may be further risks associated with transferring the task of this preliminary filtering to the EU Centre. If the Centre filters out content which is, in itself, not criminalised, but which upon evaluation, including a criminological assessment, constitutes material which indicates certain inclinations (known as “preference material”), relevant intelligence for law enforcement is likely to be lost.

5) According to Article 10 of the draft CSAM Regulation, providers of hosting services and providers of interpersonal communications services that have received a

detection order are to install and operate technologies to detect the solicitation of children with abusive intentions ("grooming"). Are you aware of technologies that can reliably distinguish between unobjectionable sexual or romantic communication and grooming?

The Cybercrime Centre and Contact Point of North Rhine-Westphalia is not aware of any such technologies in the field of research for which it is responsible. The Cybercrime Centre has been testing semantic text comprehension technologies and these tests have produced interesting approaches which can certainly be explored further, but these approaches should not be expected to reach an acceptable quality for practical implementation in the short or medium term.

6) What technical approaches do you believe offer effective, rights-compliant alternatives to the measures set out in the draft Regulation?

Please see section 1 of my comments in response to question 3. Rather than far-reaching interference in end-to-end encrypted communication infrastructures using a merely risk-based approach, the focus should mainly be on targeted investigative measures, based on a concrete initial suspicion that an offence has been committed. In addition, hash-based, server-side scanning is advisable in the case of unencrypted user content.

A complementary measure which should be considered is the implementation of a sound legal basis for the effective and complete removal and deletion of illicit content – rather than simply blocking access to it – where national legal systems do not provide for such a legal basis in their law of criminal procedure.

7) The Commission's proposal includes a call for mandatory age verification. Where exactly, and in what circumstances, would internet users have to verify their age under this proposal, and what technical options exist or are currently being explored to implement age verification in a rights-compliant manner that preserves the anonymity of users online?

My organisation has no particular expertise on the question of the design of age verification and the technical approaches relating to this. From the perspective of a technical agency that heavily uses open-source software, attention should be drawn to the implications of mandatory age verification for the open-source ecosystem. If the term "app store" is interpreted broadly, it is likely to be all but impossible for Linux distributions, for example, to navigate mandatory age verification with legal certainty. There is thus a risk that interference in the distribution system will result in significant collateral damage for law enforcement practice itself.

8) The Commission's proposal would make it possible for private communications services to be required to comply with detection orders, including to obtain content from private and encrypted chats (for example through client-side scanning) to detect grooming or for the purpose of age verification; the technology-neutral approach means that access blocking is potentially also conceivable. What would the international consequences be of such means of analysing user behaviour or restricting access to online content and safe spaces – especially regarding the higher risk of illegal foreign encroachments on European citizens' privacy (hacking), and regarding authoritarian regimes' use of the EU rules as a blueprint for illegitimate surveillance measures that are not constrained by the rule of law?

There is a risk that the techniques used to implement detection orders could be misused. This applies, firstly, to "insiders" who – for criminal reasons or on behalf of third countries – misuse access to user content; criminological experience suggests this risk should not be

overlooked. From a technological perspective, any form of client-side scanning undermines the protection offered by end-to-end encryption. The necessary interfaces on users' devices or in the software installed on them can be misused. It is true that the Commission's proposal has been worded in technology-neutral terms, and so it is currently very difficult to offer even a vague estimate of the risks. However, law enforcement practice confirms the theory that the introduction of technical risks will result, sooner or later, in the system being compromised: what can be hacked will be hacked. It can therefore be assumed that there will be a greater risk in terms of information security.

My organisation has no particular expertise on what signal would be sent to authoritarian countries.

9) The Child Rights International Network recently underlined in a study the importance of "mov[ing] beyond a privacy versus protection framing if we are to ensure that all children's rights are protected". What approach does the European Commission's current proposal take to the right of children and young people to privacy and secure IT systems, and what short-term and long-term consequences would the Commission's proposal have in this context?

My organisation has no particular expertise on this, and so I will refrain from expressing a definite view on the subject. The fact that "privacy" need not be an obstacle to "child protection" has already been made clear in section 1 of my comments in response to question 3. Regarding the effects on the IT security of systems used by children, please also see my response to question 8.

10) In your view, what package of political measures would, taken together, offer a promising approach to tackling sexual violence against children in an effective and rights-compliant manner? Where is there potential for adjustments and improvements in the field of prevention and in tackling sexual violence and online material depicting it?

Political measures should be considered, firstly, to strengthen law enforcement agencies. The actual use of financial, technical and human resources is no small factor in determining the effectiveness of efforts to combat child abuse and the dissemination of abuse material online. Please therefore see section 1 of my answer to question 3. At the same time, the improvements in the ability of law enforcement agencies to take action – as can be seen in the case of the Cybercrime Centre and Contact Point of North Rhine-Westphalia – show the effectiveness of providing resources for this.

As far as national legislation is concerned, the successor to data retention should be regarded as a significant problem. The ability to attribute IP addresses to connections or devices is an important investigative tool in combating online child abuse. Without wishing to push the boundaries of the question, given the major implications of this issue for society and for legal policy, it is likely to be advisable to implement a smart, rights-sensitive strategy which moves away from the traditional data retention approach that has been rejected by the European Court of Justice and towards limited IP attribution. Access to relevant data for investigations should take place solely in digital form, via corresponding interfaces created by the providers; this would speed up the process so that, in the case of account-related abuse offences, which are a common occurrence, current IP data can be obtained live without subsequently being stored. For the rest of this field of crime, this "log-in trap" approach should be supplemented by the possibility of storing IP attribution data for a very limited and thus rights-sensitive period, for example a week, the same duration for which data can currently be stored for the purpose of network security and resolving technical problems. This kind of new system of limited IP attribution would be a rights-sensitive, but largely practical

contribution to improving the investigative options in relation to child abuse and the dissemination of abuse material online.

At European level, an improvement in international cooperation is urgently recommended. Such cooperation offers potential and synergies that are currently not being leveraged to the necessary extent. Please also see section 2 of my response to question 3.

11) Does the European Commission's proposal effectively cover all online platforms on which child pornography material can be disseminated, and if not, what kind of improvements are potentially needed regarding the proposal's scope of application?

Please see my answers to questions 2 and 3. An approach which targets only specific platforms – setting aside the difficulty of establishing suitable criteria to determine which platforms, and the fact that practical experience shows that nearly all platforms are also used in the context of crime – is, given the concerns that have been expressed about the necessity and suitability of detection orders, in particular, neither suitable nor sufficient to compensate for the constitutional shortcomings of the Commission's proposal.

12) Does the European Commission's proposal give sufficient consideration to instruments to improve prosecution and enforcement? Where are improvements potentially needed, and what instruments would be necessary for this purpose?

Please see my answers to questions 3, 6 and 10.

13) Will the new EU Centre be able to adequately support national law enforcement agencies and Europol, according to the current plans, and what resources would it require to do so?

My organisation is expressly in favour of an improvement in international cooperation at European level. In the view of law enforcement agencies, the current plans for general surveillance of digital communications, without a reasonable suspicion of wrongdoing, are ultimately not a fully legally compliant instrument to improve prosecution and enforcement. It seems preferable for the EU Centre to be given the role of an expertise and coordination hub. Please see section 2 of my answer to question 3.

From the perspective of law enforcement agencies, which are already under-resourced today, this makes an increase in staffing levels essential at national level as well; otherwise, it seems unlikely that the Member States' law enforcement agencies will have sufficient resources, and in particular sufficient suitable staff who they will be able to second to work at the EU Centre. Please see section 1 c) of my response to question 3.

14) In your opinion, does the European Commission's proposal encompass all technical approaches which can be used to achieve the aim of protecting children, and what other technical approaches would be necessary, in your view?

Please see my response to questions 3 and 6.

15) The draft Regulation also provides for the possibility of blocking access to individual URLs, and changes to the proposal during the Czech Presidency of the Council even seek to further expand this possibility. Given the widespread use of https encryption for URL requests, do you believe it is technically feasible to specifically block individual URLs without resorting to blocking entire domains? If so, how is this possible, and if not, can this kind of access blocking comply with the requirements established by the European Court of Justice as regards the targeting of access blocking?

Law enforcement practitioners have limited experience of access blocking to date. The Code of Criminal Procedure does not provide for this kind of instrument. From a technical perspective, such measures are easy to circumvent. If the question refers to access blocking at the level of German or national access providers, I am not aware of any effective mechanism “below” the domain level. From a law enforcement perspective, blocking is in any case inadequate, because rather than restricting access to illicit content, the content should be deleted and the people disseminating such material should be prosecuted. The principle should be: “prosecute rather than just blocking access”.

16) What is your view of the role and nature of the planned EU Centre envisaged by the draft EU Regulation, firstly with regard to the performance of primarily preventive tasks, and secondly with regard to tasks relating to the development and use of technical surveillance tools?

Regarding what the role of the EU Centre should be, please see section 2 of my answer to question 3. If this question is referring to a potential credibility problem for the EU Centre regarding its preventive tasks, the preventive tasks are unlikely to be hindered by its responsibilities relating to the development and use of “technical surveillance tools”. The example of the police shows that crime repression can take place alongside prevention. The key is for both tasks to be carried out in a proportionate manner that is accepted by society. Apart from that, it should be safe to assume that suitable organisational measures can be taken, given the size of the EU Centre.

17) If scanning targeted the communications taking place on devices (“chats”), rather than the devices themselves, the same issues would exist regarding the end-to-end encryption of messaging services, for example. Again, countless law-abiding citizens would end up in the sights of the authorities simply because of their use of a specific service and the corresponding software. Are you aware of software solutions that allow end-to-end encrypted communications to be read in real time or at least decrypted? Do you believe it is justifiable to use algorithms to break the confidentiality of private communications, which is guaranteed by the German constitution?

In accordance with sections 100a et seqq. of the Code of Criminal Procedure, certain technical investigative tools are permissible. What they have in common is that they are used on the basis of a reasonable suspicion of wrongdoing, if certain strict legal requirements are met. Without a reasonable suspicion of wrongdoing, “algorithmic” surveillance and breaking the end-to-end encryption of communications are likely to be disproportionate. Please see section 1 of my answer to question 3.

18) The draft Regulation states that the EU Centre on Child Sexual Abuse to be established in The Hague is to generate binding indicators of sexual abuse material, which are to be used by the companies carrying out the scanning. Yet experienced investigators know that it is impossible to unequivocally define and substantiate on a case-by-case basis what criteria determine what constitutes a family photo, a self-documented game among children and young people, a chance snapshot of a sporting event, or, indeed, child pornography. Is any information already available about the methodology used by the EU Centre? And if so, can this methodology be regarded as reliable and suitable?

My organisation has no information about the methodology used by the EU Centre – especially prior to its establishment. A distinction is likely to be made between known abuse material that has already been categorised as such, and the detection of unknown but relevant content. In the former case, (established) techniques such as fuzzy and non-fuzzy

hashing are relevant, and maintaining relevant databases is intended to be one of the EU Centre's tasks, under Article 43 (2) b) of the draft CSAM Regulation. As far as unknown material is concerned, it seems technically possible to develop binding indicators for when content is to be considered presumably illicit, in the form of certain AI classifiers and their probability values. Unless those cases identified as being relevant are subject to human evaluation and oversight, informed by legal and criminological expertise, it is unlikely to be possible to reliably identify criminally relevant cases on the basis of AI alone.

22 February 2023

[Submitted electronically without a signature]

Markus Hartmann

Senior public prosecutor

Head of the Cybercrime Centre and Contact Point of North Rhine-Westphalia (ZAC NRW)