Does the EU need to urgently adopt the Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse online?

Summary by Alessandra Calvi (VUB/LSTS) and Juraj Sajfert (VUB/University of Luxembourg)

On 8 February 2021, the Brussels Privacy Hub, in cooperation with the **University of Luxembourg** within the framework of the FWO/FNR-funded MATIS project, and in media partnership with **Privacy Laws & Business** organised the second webinar within the series **Enforcing Europe - Webinar Series 1,** .

The second webinar, entitled **Does the EU need to urgently adopt the Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse online?** discussed the September 2020 **Proposal of the European Commission for an Interim Regulation on processing personal and other data for the purpose of combatting child sexual abuse online**, which was supposed to be adopted by the end of 2020.

Juraj Sajfert (VUB/University of Luxembourg) moderated the discussion. Invited speakers were **Cathrin Bauer-Bulst** and **Antonio Labrador Jimenez** (European Commission, DG HOME, Cybercrime Unit), **Michela Palladino** (Facebook, EU Public Policy) and **Alan Butler** (EPIC), who tackled the following questions.

- *What is Interim Regulation? What are its objectives?*
- *What kind of technologies service providers use in the fight against child sexual abuse online? How have they been affected by the entry into force of the recast European Electronic Communications Code on 21 December 2020?*
- *What are the practical consequences of the non-adoption of the Interim Regulation by 21 December 2020? How do we move forward? Does the Interim Regulation set a precedent?*

Antonio Labrador Jimenez emphasised that the interim Regulation is a key tool to protect children victims of online sexual abuse, pending the negotiations on the e-Privacy Regulation.
As the entry into force of the recast European Electronic Communications Code extended the scope of the e-Privacy directive to 'over the top' inter-personal communication services, providers (of number-independent interpersonal communication) were unable to lawfully continue using well-established techniques such as hashing technologies to combat online child sexual abuse. The Interim Regulation waives from certain obligations under Directive 2002/58/CE, allowing providers, on a voluntary basis, to continue using technologies to prevent, detect, report child sexual abuse online, other than removing illicit materials. The Interim Regulation does not introduce new legal basis for processing, but preserves the *status quo,* whilst a proposal for a new and comprehensive solution n is expected for the summer 2021.

Michela Palladino noted how the Interim Regulation contains provisions that create unrealistic expectations from the service providers. For example, the Interim Regulation does not allow processing and storing traffic data and metadata; sets unrealistic maximum error rates for the technologies scanning communications; requires suspicion of child sexual abuse before scanning private communication (whereas normally it is by scanning communication that a suspicion emerges). She called for EU legislators to consider the importance of traffic data and metadata for combatting child sexual abuse online in the upcoming legislation.
Albeit Facebook stopped using Artificial Intelligence and Machine Learning to proactively detect nudity and videos from private communications to comply with the e-Privacy Directive, they continued using

such technologies in non-encrypted services, as well as in public communication. She added that users' reports are also important tools to detect harmful content and accounts.
Together with the law, Facebook policies and community standards (introducing e.g. age limit to use the platform, forbidding the publication of content endangering children, limiting the number of interactions that teenagers can have) constitute the main basis of their content moderation worldwide.

Alan Butler stated that in the United States most cases of child sexual abuse online are framed under the Fourth Amendment, which protects individuals against unreasonable searches and seizures from governmental intrusions, and the so-called private search doctrine. Under the private search doctrine, when a private entity conducts a search, and inform the government of what it has found, the government can repeat the search without first obtaining a warrant and make use of that information if there is a "virtual certainty" that the scope of the government search will not exceed that of the private search. Referring to a recent case where EPIC filed an *amicus* letter, he argued that whereas for 'physical' searches and seizures the evaluation of the scope of public and private searches is easier, automation adds a layer of complexity. Unless the government provides evidence about the accuracy and reliability of the technologies used, the evaluation of the "virtual certainty" is not possible. He added that whereas an affirmative duty to scan communications is introduced, this will change how courts address the topic.

In the Q&A, several concerns were raised. It was questioned if the current voluntary practices to detect and report child sexual abuse were legal, and how this could affect both the interim and long-term legislation. It was noted how Courts and Data Protection Authorities (DPAs) consider such practices. An attendee reported that a complaint was filed with the Schleswig-Holstein DPA against the practice of large US corporations to generally and indiscriminately search the content of all private user messages to detect child sexual abuse. Concerns were expressed that the lack of resources of DPAs could avail the use of intrusive technologies, as well as uncertainties about the coordination among DPAs and National Regulatory Authorities (NRA) under the Code. Facebook was urged to increase the resources in terms of personnel devoted to content moderation.
Questioned about the role of data protection impact assessment of algorithms used to fight child sexual abuse online, Alan Butler stated that, in the US, it is unlikely that government authorities perform an independent assessment of algorithms used by companies, adding that also courts are not adequately scrutinising them. Cathrin Bauer-Bulst claimed that for technologies such as hashing techniques that detect previously reported sets of images and videos depicting abuses, DPIA is less relevant. Conversely, it becomes crucial in the case of machine learning. She emphasised the importance of including a human in the loop, especially considering that certain contents (e.g. manga) are criminalised in certain jurisdictions and not in others. She added that in some cases technologies just give suspicion of child sexual abuse, being up to law enforcement authorities to decide how to proceed.