CISPE.cloud

CISPE voices serious concerns on proposed EU terrorist content legislation: ‘The European Commission is targeting the wrong players’

“Europe’s cloud infrastructure service providers are being asked to do the impossible: it’s like asking the power company to turn off a single light bulb in an apartment without shutting down the entire apartment block or city.”

***Brussels, 27/11/2018* – CISPE, the alliance of Cloud Infrastructure Services Providers in Europe, is raising major concerns about the scope of the European Commission’s proposed Regulation covering terrorist content online. CISPE believes the Regulation, which asks infrastructure providers to scan and monitor all enterprise data running across there services, is targeting the wrong players, slowing down their digital transformation and immediately bringing to a halt the protections of the General Data Protection Regulation (GDPR).**

“CISPE and its members support the intention of the Regulation and already fully co-operate with judiciary authorities and court orders to fight terrorism content,” says Alban Schmutz, CISPE Chairman and VP Strategic Development & Public Affairs, OVH. “However, including cloud infrastructure providers in the legislation means the wrong players are being targeted.”

“Unlike social media platforms, video and other *online content sharing* services that have control down to the most granular piece of content made available on their platforms by their users - these are the primary targets of the Regulation - cloud infrastructure providers have **no** control or access to the data stored by their customers, or over how and when such data is made available to the public.

Cloud infrastructure users include corporations (banks, insurers, lawyers, transport, energy) and governments (public agencies, hospitals, law enforcement, etc.), that do not typically make content available to the public. Indeed, infrastructure providers cannot even distinguish between what is “a piece of content” and what is not “a piece of content”. If an infrastructure customer is hosting social media or a website sharing content from 1,000,000 users and one user uploads a piece of illegal content, like a photograph, the infrastructure provider would be forced shut down the entire social media service or website, which is simply not feasible.

Concerns also exist on the imposition of “automated proactive measures” (Article 6) to monitor or prevent uploads of terrorist content. For cloud infrastructure providers, this is simply not possible. Moreover, if such technologies were developed in the future, infrastructure providers would be required to monitor all data entrusted to them by individuals, corporations and public institutions - even when such data is not available to the public.

Alban Schmutz adds, “Such measures would require accessing every single data owned by infrastructure customers – which could include law enforcement emails, sensitive intellectual property like design files of an aircraft, genomic databases, power plants operations and so on - therefore undermining the security and confidentiality of sensitive content that were never intended to be available to the public.”

CISPE believes that in its current form, the Regulation poses a serious threat to the core assets of cloud infrastructure customers (European industries, services and governments), thereby slowing down their digital transformation and immediately bringing to a halt the protections of the General Data Protection Regulation (GDPR) that only came into force six months ago.

CISPE is urging the legislators to clarify the scope of the proposed Regulation, to exempt cloud infrastructure services providers, and include rules that are clear, workable and proportionate.

Link to CISPE position paper

Contact: to speak to CISPE or a member please email cispe@europa-insights.com or call +32 2 502 65 80

Notes to Editors: Unlike the filtering ‘hashing recognition’ technology used by social, video, image or audio sharing platforms, which creates a digital fingerprint of content that must be already identified (and made available to the public at least once) so the same content is not re-uploaded in another platform, cloud infrastructure providers are **not technically able** to use such technology since they do not have visibility or access over the content.

About CISPE: The association is open to all companies, no matter where they are headquartered, provided they declare that at least one of their cloud infrastructure services meets the requirements of the CISPE Data Protection Code of Conduct. The CISPE Code of Conduct already has more than 100 services declared, provided by 30+ cloud enterprises headquartered in more than 15 EU Member States and used by millions of businesses across Europe.

CISPE Executive Board https://cispe.cloud/board-of-directors/

Cloud Computing Services declared under CISPE Code of Conduct https://cispe.cloud/publicregister/