Di

Il CISPE solleva serie preoccupazioni sulla legislazione proposta dall'Unione europea contro i contenuti terroristici:
"La Commissione europea sta sbagliando bersaglio"

"Ai provider di servizi di infrastrutture cloud europei viene chiesto l'impossibile: è come chiedere a una compagnia elettrica di spegnere una singola lampadina in un appartamento senza togliere energia all'intero condominio o a tutta la città".

Bruxelles, 27/11/2018 – Il CISPE, associazione dei provider di servizi cloud che operano in Europa, sta sollevando serie preoccupazioni sull'ambito di applicazione della Direttiva proposta dalla Commissione europea in materia di contenuti online di tipo terroristico. Il CISPE ritiene che la Direttiva stia colpendo il bersaglio sbagliato, in quanto chiede ai provider di infrastrutture di analizzare e monitorare tutti i dati aziendali circolanti nei loro servizi, cosa che non è tecnicamente possibile.

"Il CISPE e i suoi membri supportano l'intenzione della Direttiva, infatti collaborano pienamente con le autorità giudiziarie e rispettano le ordinanze dei tribunali per contrastare i contenuti terroristici", afferma Alban Schmutz, Presidente del CISPE e Vice Presidente per lo Sviluppo strategico e gli Affari pubblici di OVH. "Tuttavia, includere i provider di infrastrutture cloud nella normativa significa colpire il bersaglio sbagliato".

"Diversamente dalle piattaforme di social media, video e altri servizi di *condivisione di contenuti online,* che hanno il pieno controllo di ogni singolo frammento di contenuto reso disponibile sulle loro piattaforme dagli utenti, che rappresentano il bersaglio principale della Direttiva, i provider di infrastrutture cloud **non** possono accedere ai dati conservati dai propri clienti né controllarli o vigilare quando e sul modo in cui essi vengono resi disponibili al pubblico. Quello che la Direttiva chiede a noi è come chiedere a un meccanico della società che gestisce le autostrade di riparare ogni singola auto difettosa che percorre un suo tratto di strada".

Fra gli utenti delle infrastrutture cloud ci sono grandi società di capitali (bancarie, assicuratrici, legali, del settore dei trasporti e dell'energia) e governi (enti pubblici, ospedali, forze dell'ordine ecc.) che generalmente non rendono i propri dati disponibili al pubblico. Proprio per questo i provider di infrastrutture non possono neanche distinguere tra cosa costituisce una "parte di contenuti" e cosa non lo è. Se un cliente conserva in un'infrastruttura contenuti di social media o i contenuti condivisi su un sito web da 1.000.000 di utenti e un singolo utente effettua l'upload di una parte di contenuti illegali, come una fotografia, il provider dell'infrastruttura sarà obbligato a eliminare l'intero servizio di social media o sito web.

Le perplessità riguardano anche l'imposizione di prendere "misure automatizzate proattive" (Articolo 6) per monitorare o prevenire l'upload di contenuti a carattere terroristico. Per i provider delle infrastrutture cloud, ciò non è tecnicamente possibile. Inoltre, anche qualora tali tecnologie venissero sviluppate in futuro, i provider di infrastrutture dovrebbero spiare tutti i dati consegnati loro sulla base di un rapporto di fiducia da persone fisiche, società di capitali e istituzioni pubbliche, anche se tali dati non sono di dominio pubblico.

Alban Schmutz aggiunge: "Tali misure obbligherebbero ad accedere a tutti i dati posseduti dai clienti dell'infrastruttura, il che potrebbe includere e-mail contenenti ordinanze giudiziarie, proprietà intellettuali sensibili, come i file riguardanti la progettazione di un aereo, database genomici, il funzionamento di centrali elettriche e così via. Pertanto, ciò minerebbe la sicurezza e la riservatezza di contenuti sensibili la cui diffusione pubblica non era mai stata prevista".

Il CISPE ritiene che, così com'è, la Direttiva rappresenti una seria minaccia per le risorse principali dei clienti delle infrastrutture cloud (aziende, servizi e governi europei), rallentando così la loro trasformazione digitale e ponendo un freno al Regolamento generale sulla protezione dei dati (GDPR) entrato in vigore appena sei mesi fa.

Il CISPE esorta i legislatori a chiarire il campo di applicazione della Direttiva proposta, a esentare i provider di servizi di infrastruttura cloud e a includere regole chiare, realizzabili ed equilibrate.

Link al documento di sintesi del CISPE

Contatti: per parlare con il CISPE o un suo membro, inviare un'e-mail a cispe@europa-insights.com o chiamare il +32 2 502 65 80

Note per gli editori: A differenza della tecnologia di filtraggio 'hashing recognition' utilizzata dalle piattaforme di condivisione social, di video, immagini o audio, che crea un'impronta digitale di contenuti che devono essere già identificati (e messi a disposizione del pubblico almeno una volta) affinché non siano oggetto di upload su un'altra piattaforma, i provider di infrastrutture cloud **non** sono **tecnicamente in grado** di utilizzare tale tecnologia in quanto non possono vedere né accedere ai contenuti.

Informazioni sul CISPE: All'associazione possono partecipare tutte le aziende, indipendentemente da dove è ubicata la loro sede centrale, purché dichiarino che almeno uno dei loro servizi di infrastruttura cloud soddisfi i requisiti del Codice di condotta sulla protezione dei dati del CISPE. Ad oggi il Codice di condotta del CISPE ha raccolto l'adesione di oltre 100 servizi, forniti da più di 30 aziende cloud con sede centrale in oltre 15 Stati membri dell'Unione europea e già utilizzati da milioni di imprese in tutta Europa.

Comitato esecutivo del CISPE https://cispe.cloud/board-of-directors/

Servizi di cloud computing dichiarati aderenti al Codice di condotta del CISPE https://cispe.cloud/publicregister/