Soro ‘Normalizzare l’allarme terrorismo è un danno alla privacy’

In quest’epoca di terrorismo immanente diversi Paesi, dagli Stati Uniti alla Francia fino all’Italia, in nome della ‘sicurezza nazionale’ stanno limitando per anni, e non più per un breve periodo, i diritti e le libertà dei cittadini. L’allarme è stato lanciato dal Garante Privacy, **Antonello Soro**, nell’intervento tenuto, questa mattina nella sala Zuccari del Senato, in occasione della presentazione del report ‘*Sorveglianza da parte dei servizi di intelligence: garanzie dei diritti fondamentali e mezzi di ricorso nell’UE. Prospettive e aggiornamento normativo’* curato dall’Agenzia dell’Unione europea per i diritti fondamentali (**FRA**).

“*La vera sfida di oggi consiste nel rendere la tecnologia una risorsa tanto per la sicurezza quanto per le libertà*” ha affermato Soro, senza dunque mettere nell’angolo i diritti fondamentali di una democrazia. E il rischio da evitare, ha ammonito il Garante, “*nell’attuale contesto di terrorismo immanente è quello di normalizzare l’emergenza e, con essa, la compressione dei diritti e delle libertà che ne consegue*”.
Il presidente dell’Autorità per la protezione dei dati personali ha tenuto l’intervento alla presenza, tra gli altri, del Presidente del Copasir, il senatore **Giacomo Stucchi** e di **Alessandro Pansa**, direttore generale del Dipartimento delle informazioni per la sicurezza (DIS).

Soro, focalizzando il suo discorso sul rapporto libertà e sicurezza, ha anche illustrato la strategia migliore per fronteggiare il terrorismo senza penalizzare, per tanti anni o peggio ancora per sempre, la privacy dei cittadini, perché “*neanche la sicurezza nazionale è una zona totalmente ‘franca’, in cui si possano violare impunemente i principi*

generali del diritto europeo”.

Ecco dunque le indicazioni del Garante Privacy:

“Per il contrasto del terrorismo bisogna essere ‘più efficaci, non meno liberi”. Ed essere più efficaci vuol dire soprattutto coordinare l’azione investigativa, ha spiegato Soro, ciò che pare sia mancato spesso negli ultimi anni in molti Paesi europei, e adeguare il diritto a quella tecnologia in continua evoluzione, che è una delle risorse strategiche dei terroristi. Ma tutto questo senza illudersi di poter delegare a un algoritmo le strategie di indagine, ha messo in guardia il Garante, che devono basarsi su di una raccolta selettiva, non “a strascico”, dei dati personali e sull’ineliminabile “fattore umano”, capace esso solo di dare senso ai **Big Data**.

‘Il modo migliore per difendere la nostra sicurezza è proteggere i nostri dati’

Antonello Soro, consapevole che il mondo sta vivendo una nuova stagione del terrorismo, con *“la costanza, l’efferatezza, l’ubiquitarietà delle azioni jihadist”,* ha tuttavia messo in evidenza le conseguenze negative sulla privacy e sulle libertà in generale dei cittadini statunitensi e francesi, e di chi visita questi Stati, a seguito delle norme varate dopo gli attentati, a partire dall’11 settembre 2001: *“Emblematico l’esempio americano, ove a distanza di oltre 16 anni da Ground Zero e meno di tre anni dopo le riforme, più garantiste, di Obama, si tornano a conferire all’intelligence ampi poteri di sorveglianza massiva, con vagli giurisdizionali limitatissimi, solo successivi e peraltro eventuali”.*

L’allarme terrorismo è stato normalizzato anche in Francia: *“dove, al di là del progetto di codificare l’emergenza in Costituzione”,* ha ricordato Soro, *“sono state recentemente approvate norme di contrasto del terrorismo fortemente limitative delle libertà individuali e ad applicazione non più temporanea ed eccezionale ma ordinaria”.*

Il concetto chiave è questo per capire come bilanciare il rapporto sicurezza e privacy? Quest'ultima può essere limitata, compressa, in nome della sicurezza nazionale, ma solo per un determinato periodo di tempo e in via eccezionale. L'intervento del Garante si basa su questo principio espresso dalla Corte di giustizia europea con il quale ha costruito l'architrave del rapporto tra strumenti investigativi e protezione dati.

In barba a questo principio e alle sentenze della Corte di giustizia europea il Parlamento italiano ha recentemente aumentato da due fino a 6 anni la Data retention, ossia dal 12 dicembre 2017 gli operatori telefonici hanno l'obbligo di conservare i dati del proprio traffico telefonico e telematico, nonché quelli relativi alle chiamate senza risposta, per il termine di 72 mesi.

Un'enormità.

E un *unicum* in Europa.

I problemi di privacy legati a questa legge sono diversi, ma pensiamo a uno, potenzialmente, molto grave: un attacco hacker andato a buon fine ai server degli operatori telefonici in cui sono immagazzinati i traffici telefonici e su internet di milioni di italiani. Per scongiurare questo rischio sarebbe meglio evitare le raccolte massive dei dati, limitando dunque "la superficie d'attacco" per un terrorismo che sempre più si alimenta della rete.

Per questo ha ragione Antonello Soro nel dire che '*il modo migliore per difendere la nostra sicurezza è proteggere i nostri dati'.*

Per approfondire:

> *Soro 'Normalizzare l'allarme terrorismo è un danno alla privacy'*