PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4851 di Lunedì 18 gennaio 2021

Le regole per l'accesso ai dati del traffico telefonico

Una sentenza della corte di giustizia dell'Unione Europea stabilisce le regole per la conservazione di dati afferenti al traffico telefonico.

Più volte le forze dell'ordine hanno potuto rendere più incisiva la loro azione, a difesa della società civile, analizzando il traffico telefonico di soggetti sotto sorveglianza. A fronte di alcuni eccessi, che si sono verificati in alcuni paesi europei, la corte di giustizia ha stabilito regole precise per l'accesso a questi dati.

La corte di giustizia dell'unione europea ha emesso una sentenza, applicabile ad alcuni contenziosi posti alla sua attenzione, afferenti all'obbligo, da parte di un gestore di servizi di comunicazioni elettroniche, di conservare e comunicare dati di traffico, compresi dati di tracciamento, alle forze dell'ordine.

Come, a fronte di una rapina in una banca, automaticamente le forze dell'ordine richiedono copia delle immagini riprese dagli impianti di videosorveglianza dell'intera via, dove si trova l'agenzia bancaria, e le vie adiacenti, le forze dell'ordine richiedono sistematicamente dati di traffico e geo localizzazione afferenti a soggetti sotto controllo, nell'ambito di indagini penali. Evidentemente questa abitudine, in vari paesi europei, ha superato i limiti di compatibilità con le vigenti leggi europee ed è questa la ragione per la quale la corte di giustizia ha ritenuto opportuno emettere una sentenza, che accorpa procedimenti aperti in vari paesi.

In particolare, la corte ha stabilito che la conservazione e trasmissione di questi dati alle forze dell'ordine, a fronte di un generico impegno nel contrasto alla criminalità o per ragioni afferenti alla sicurezza nazionale, non è lecita.

Perché questo trasferimento di dati avvenga lecitamente, occorre rispettare dei criteri assai più restrittivi, ad esempio legati a concrete e gravi minacce alla sicurezza nazionale. Per quanto riguarda le attività di contrasto alla criminalità, la trasmissione dei dati deve avvenire in un contesto di garanzie di protezione e, soprattutto, solo dopo che un magistrato, od un'autorità amministrativa indipendente, ha emesso un provvedimento autorizzatorio.

Questa sentenza è particolarmente importante, perché finalmente stabilisce un confine fra il più che giustificabile desiderio delle forze dell'ordine di avere a disposizione il massimo numero possibile di elementi indiziari e probatori, e la necessità di rispettare le vigenti leggi europee in materia di protezione dei dati personali, che stabiliscono il principio generale di minimizzazione della raccolta e conservazione dei dati.

Ecco perché, anche se alcuni paesi avevano pubblicato provvedimenti legislativi in merito all'utilizzo di questi dati, la corte ritiene che ciò non sia sufficiente, ma sia richiesto un più approfondito studio circa le esigenze di conoscenza dei dati e, soprattutto, una valutazione indipendente, da parte di un magistrato.

In particolare, la corte ha ricordato che l'articolo 23, comma 1 del regolamento generale sulla protezione dei dati deve essere interpretato in modo compatibile con la dichiarazione universale dei diritti dell'uomo e pertanto tale articolo proibisce ai legislatori nazionali di emettere disposizioni legislative eccessivamente invasive.

Nei casi eccezionali, laddove quindi ci si trovi in presenza di una seria minaccia alla sicurezza nazionale, è possibile derogare al divieto, ma solo per un periodo di tempo limitato e sempre dietro autorizzazione di un rappresentante della magistratura.

Un ragionamento similare si applica alla conoscenza degli indirizzi IP, che vengono assegnati ai soggetti coinvolti in una comunicazione elettronica, sempre però introducendo un esplicito limite di durata di conservazione.

L'estensione della durata di conservazione può essere giustificata, sempre con l'autorizzazione di un magistrato, quando gli elementi probatori acquisiti sono sufficientemente concreti.

Tutte queste deroghe sono particolarmente applicabili a scenari terroristici, a dimostrazione dell'attenzione sempre crescente che l'Europa pone a questo fenomeno, che dovrebbe essere messo sotto controllo in via preventiva, piuttosto che dopo il verificarsi di qualche tragedia.

Infine, la corte mette in evidenza come, ove un procedimento penale in una nazione sia stato avviato sulla base di dati non correttamente acquisiti, sia dati relativi alle comunicazioni, sia al tracciamento dei soggetti coinvolti, il tribunale coinvolto dovrebbe ignorare questi elementi probatori.

Court of Justice of the European Union - PRESS RELEASE No 123/20 (PDF)

Adalberto Biasiotti