NORME E TRIBUTI Il Sole 24 Ore 05 NOVEMBRE 2024

OSSERVATORIO SU GIUSTIZIA E DIGITALE

Il controllo giudiziario sull'accesso ai dati tutela e garantisce i diritti

Federica Paulicci e Oreste Pollicino

A margine dello scandalo che ha acceso il dibattito — non solo in Italia — negli ultimi giorni, riguardante l'accesso illecito a informazioni riservate di un gruppo di oltre 800mila persone, secondo le attuali stime, la Corte di giustizia dell'Unione Europea è tornata a pronunciarsi sulle modalità di accesso ai dati personali delle persone fisiche da parte delle forze di polizia. Un tema che potrebbe apparire anacronistico, considerando la mole di informazioni reperite e la crescente complessità della tutela dei dati nell'era digitale, ma che evidenzia la necessità di una regolamentazione chiara e uniforme per proteggere i diritti fondamentali dei cittadini.

Ebbene, il caso C-548/2021 che è stato sottoposto all'attenzione dei giudici europei ha riguardato un tentato accesso da parte della polizia austriaca allo smartphone di un individuo sospettato di detenere 85 grammi di cannabis. Difatti, durante la perquisizione, gli agenti hanno richiesto l'accesso ai dati memorizzati sul cellulare dell'indagato il quale si è però rifiutato di sbloccare il dispositivo. Dopodiché gli agenti hanno sequestrato il suo telefono, che conteneva una scheda sim e una scheda sd, senza la preventiva autorizzazione di un pubblico ministero o di un tribunale. Di seguito, la polizia ha effettuato diversi tentativi di accedere ai dati del cellulare. Constatato l'insuccesso, il dispositivo è stato successivamente trasferito all'Ufficio federale di Investigazione criminale di Vienna per ulteriori tentativi di aggirare la sicurezza del telefono. Solamente quando il telefono gli è stato restituito, l'indagato è venuto a conoscenza dei tentativi di accesso ai suoi dati. Ha, quindi, depositato un ricorso sostenendo che queste azioni hanno violato i suoi diritti alla privacy in base al diritto dell'Ue. Si badi bene, dalla ricostruzione della sentenza, sembrerebbe che la polizia non abbia avuto accesso ai contenuti del telefono.

In primo luogo, la Corte ha rammentato che il principio di minimizzazione dei dati, sancito dalla direttiva 2016/680 (nota come *Law enforcement directive* o Led), impone che le autorità raccolgano solo i dati adeguati, pertinenti e non eccedenti rispetto all'indagine specifica. Questo principio mira a garantire che la raccolta di dati sia sempre proporzionata, in qualità e quantità dei dati, nonché rispettosa dei diritti individuali. Pertanto, nel caso di specie, l'accesso ai dati dell'indagato sarebbe permesso purché nel rispetto di queste garanzie.

Inoltre, un altro elemento cruciale riguarda i requisiti per l'autorizzazione alla raccolta di dati e all'uso di strumenti tecnologici per lo svolgimento delle indagini.

Il caso, difatti, mette in discussione se la legge austriaca, che permette alle forze dell'ordine di accedere ai dati digitali senza un'autorizzazione giudiziaria o amministrativa preventiva, sia in linea con le norme europee.

In particolare, si solleva la questione se sia legittimo permettere tale accesso per reati minori, punibili con una pena detentiva massima di un anno, senza le dovute garanzie procedurali. Le disposizioni dell'Unione Europea richiedono infatti garanzie procedurali, tra cui controlli di supervisione e valutazioni di proporzionalità, per proteggere la privacy delle persone, specialmente quando si tratta di reati meno gravi, come quello in esame.

La Corte ha rammentato, quindi, che l'assenza di un controllo giudiziario preventivo è in contrasto con i diritti fondamentali, specie l'articolo 47 della Carta, che è garanzia del principio del giusto processo, tutelando gli individui della possibilità di contestare decisioni che incidono sui propri diritti, giacché, di contro, si compromette il loro diritto a un ricorso effettivo e alla trasparenza. È, pertanto, fondamentale garantire che l'accesso ai dati sia proporzionato alla gravità del reato e soggetto a un controllo adeguato.

Questo aspetto è di grande attualità anche per quel che concerne l'applicazione dell'*Artificial intelligence act*. Il regolamento, tra le altre cose, stabilisce delle norme specifiche per l'utilizzo di sistemi di riconoscimento biometrico da parte delle forze dell'ordine. In particolare, la norma prevede che qualsiasi utilizzo di tali sistemi deve ricevere un'autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente. Questa disposizione è fondamentale perché definisce le modalità di regolamentazione e controllo delle tecnologie di IA che hanno un impatto significativo sui diritti individuali. Questa scelta spetta chiaramente agli Stati membri e deve essere presa entro novembre 2024.

In attesa di conoscere cosa farà l'Italia, è essenziale ricordare, anche alla luce del caso in esame, che la scelta tra controllo giudiziario e amministrativo non è meramente procedurale, ma ha implicazioni significative sul modo in cui i sistemi di IA vengono governati e sul livello di controllo che ricevono. La supervisione giudiziaria offre un livello di protezione giuridica più elevato, garantendo che l'impiego delle tecnologie di IA sia sottoposto a standard giuridici rigorosi che danno priorità ai diritti fondamentali. D'altro canto, se da un lato la supervisione amministrativa può garantire efficienza, dall'altro può mancare dello stesso livello di responsabilità e trasparenza. I giudici sono responsabili dell'interpretazione e dell'applicazione delle tutele dei diritti fondamentali, garantendo che l'uso dei sistemi di IA sia giustificato e conforme agli standard legali stabiliti.