Privacy, corrispondenza e repressione dei reati: c'è spazio per un ménage à trois?

di Giulio Rivellini - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 24 gennaio 2024

L'Online Safety Act è stato recentemente approvato nel Regno Unito e sembra delineare un internet "su misura" per i cittadini inglesi. Pensata per disciplinare i servizi online "user-to-user", tale legge rischia di aprire una breccia nella privacy degli utenti, obbligando astrattamente i providers a scansionare i messaggi dei loro clienti per intercettare, prevenire e reprimere i reati legati al terrorismo e all'abuso e sfruttamento minorile. Spetta ora a Ofcom trovare le soluzioni tecniche per garantire il rispetto dei diritti degli utenti e, al contempo, raggiungere gli obiettivi imposti dal legislatore inglese.

È possibile coniugare privacy, tutela della corrispondenza e repressione dei reati? Si può fare, secondo il Regno Unito. Westminster ha infatti recentemente approvato l'***Online Safety Act***, una legge volta a disciplinare, tra le altre cose, l'attività dei fornitori di servizi online "**user-to-user**" ("u2u"), tra i quali rientrano anche i più noti colossi della messaggistica. Si tratta di un progetto ambizioso, che impone alcuni obblighi in capo ai fornitori di tali servizi e che dovrà essere attuato da Ofcom, l'autorità inglese di regolazione del settore.

L'intervento promosso dal governo inglese non è certo un caso isolato nel panorama globale. L'Unione europea si è già mossa in tal senso, imponendo specifici obblighi per i fornitori di servizi online nell'ambito del *Digital Service Act* (ne abbiamo parlato **QUI**). C'è però una disposizione, nell'*Online Safety Act*, che si spinge oltre e che ha destato particolari preoccupazioni: si tratta della c.d. "**spy clause**" (*clause 121*), che apre una possibile breccia nella privacy degli utenti.

Tale clausola permette a Ofcom di ordinare ai fornitori di servizi "u2u" di utilizzare tecnologie per **identificare contenuti terroristici** o che riguardano **l'abuso o lo sfruttamento minorile** (*Child Sexual Exploitation and Abuse*, CSEA). Si tratta quindi del potere di accedere ai contenuti degli utenti e di scansionarli per contrastare e, ove possibile, prevenire la commissione di tali reati.

La possibilità di intervenire sulla moderazione dei contenuti, imponendo un controllo a tappeto sui messaggi scambiati dagli utenti, ha sollevato diverse critiche da parte degli operatori del settore, i quali denunciano una violazione senza precedenti alla **privacy** degli utenti. Le aziende responsabili di servizi come Whatsapp, Signal, Session, Threema e Wire hanno messo in guardia il governo inglese dai possibili rischi insiti nella *spy clause*, minacciando persino di abbandonare il paese nel caso in cui tale disposizione li obbligasse a scansionare i contenuti degli utenti.

Le critiche non hanno però scalfito i propositi del legislatore inglese, il quale alla fine ha adottato l'*Online Safety Act*. Bisognerà ora attendere la sua **attuazione**, dal momento che in realtà la *spy clause* è alquanto vaga sulle tecnologie da utilizzare per monitorare i contenuti: si fa infatti genericamente riferimento a una "accredited technology" per identificare i reati. Secondo il governo inglese ciò significa che Ofcom potrà imporre la scansione dei contenuti soltanto quando sarà possibile garantire il rispetto della crittografia *end-to-end*. Seguendo questo ragionamento, però, la *spy clause* non sembra

attuabile, dal momento che è tecnicamente impossibile scansionare i messaggi senza violare la crittografia *end-to-end*. La palla quindi ora passa a Ofcom, chiamata a trovare un compromesso tra la privacy degli utenti, la segretezza della loro corrispondenza e l'interesse pubblico alla prevenzione e repressione dei reati.