EDITORIALE

Il sempre più difficile equilibrio tra Privacy e Sicurezza nazionale

Sul proprio *account* di Twitter il 16 novembre 2016 Edward Snowden commentava così la ratifica dell'*Investigatory Power Act*: "*Il Regno Unito ha appena legalizzato la sorveglianza più estrema nella storia della democrazia occidentale. Va oltre a molte autocrazie*". La legge accresce i poteri investigativi delle agenzie britanniche e **consente di obbligare i fornitori di comunicazioni a rimuovere la protezione elettronica applicata a qualsiasi comunicazione o dati**. Sulla nuova legge britannica il quotidiano The Guadian ha riportato la dichiarazione di Jim Killock, direttore esecutivo del gruppo Open Rights: "*Il Regno Unito ha ora una legge di sorveglianza più adatta a una dittatura che a una democrazia. Lo Stato ha poteri senza precedenti per controllare e analizzare le comunicazioni dei cittadini britannici indipendentemente dal fatto che siamo sospettati di un'attività criminale*". D'altra parte, si sono registrati commenti anche a favore del nuovo strumento investigativo. Jonathan Evans, ex capo del Mi5, parlando al programma di BBC Radio 4's Today, ha dichiarato: "*Io non sono personalmente uno di quelli che pensa che dobbiamo indebolire la crittografia perché ritengo che esiste un problema parallelo, cioè la sicurezza informatica […] È molto importante vivere in un paese in cui le persone possano operare in modo sicuro. È importante per i nostri interessi commerciali e per i nostri interessi di sicurezza, quindi la crittografia in questo contesto è molto positiva*".

Quella appena descritta è una tipica contrapposizione di idee, generalizzata in tutti i paesi industrializzati, riguardo l'equilibrio che dovrebbe assumere da un lato la garanzia della privacy nelle telecomunicazioni e dall'altro la sicurezza nazionale. Giova, tuttavia, ricordare che altro è la potenzialità di uno strumento, seppur investigativo, altro è la legge che la regolamenta.
Con le divulgazioni sulla sorveglianza di massa del 2013 ad opera di Snowden, l'attenzione posta dai grandi colossi del web verso la privacy è aumentata fino al livello massimo, comprendendo con questo limite anche una radicale modifica del nostro modo di navigare su Internet e di comunicare. Se da una parte oggi possiamo essere certi che la foto di nostro figlio attraversi l'intero *world wide web* per arrivare (solo) ai suoi cari nonni, dall'altra non possiamo escludere che questo livello massimo di privacy venga sfruttato anche per attività criminose, senza escludere attività diverse dal "classico" traffico di droga. Secondo quanto ha riportato il Financial Times ad agosto 2017, l'Fbi ha fornito le prime indicazioni su un uso diffuso di WhatsApp, Signal e Telegram da parte dei colletti bianchi nelle grandi banche. Infatti, in un recente caso di *insider trading*, un ex dipendente di Bank of America si è dichiarato colpevole in una frode da 5 milioni di dollari in cui, usando un'app di messaggistica telefonica, passava a tre suoi amici informazioni classificate e riservate su operazioni e acquisizioni future dell'istituto di credito.

L' *Investigatory Power Act* inglese è sicuramente il primo esempio di risposta concreta all'uso criminale dei nuovi strumenti di messaggistica cifrata, che segue gli attacchi terroristici a Rochdale del 18 febbraio 2016 e a Londra del 21 ottobre 2016. Sulla base di questa legge il governo australiano ha modellato un'analoga bozza. **Il 14 luglio 2017 l'Australia ha proposto una nuova legge sulla sicurezza in ambito informatico che obbliga le aziende tecnologiche globali, come Facebook e Google, ad aiutare la polizia a "sottrarre" messaggi crittografati inviati da sospetti estremisti ed altri criminali**. Secondo la polizia federale australiana le comunicazioni controllate criptate sono cresciute negli ultimi anni dal 3% a più del 55% e sono presenti nel 65% delle indagini sulla criminalità organizzata. Il primo ministro Malcolm Turnbull ha dichiarato che, secondo la legge australiana, le società di comunicazione su Internet avrebbero gli stessi obblighi che hanno le aziende telefoniche nell'aiutare le forze dell'ordine.

Su questo orientamento il governo australiano ha già previsto la resistenza di alcune società di tecnologia, molte delle quali hanno sede negli Stati Uniti; ma le società "*sanno moralmente che dovrebbero cooperare*", ha dichiarato Turnbull. Alcuni esperti avvertono che l'indebolimento dei servizi di crittografia end-to-end, tale per cui la polizia possa intercettare, lascerebbe le comunicazioni vulnerabili agli hacker. Turnbull ha aggiunto anche "*Dobbiamo dire con una sola voce alla Silicon Valley e ai suoi emulatori: «D'accordo, hai ideato queste grandi piattaforme, ora devi aiutare a garantire che il rispetto della legge prevalga»*" e con una sola voce invitava tutti gli Stati del G20, così come ribadito al vertice dell'8 luglio 2017 ad Amburgo dove l'Australia è stato un driver importante per la dichiarazione concordata tra i 20 leader mondiali, con la quale si invita l'industria del settore a fornire "accesso legale e non arbitrario alle informazioni disponibili" necessarie per proteggere dalle minacce terroristiche.

La Germania ha fatto proprie queste linee di principio, in quanto **il Parlamento tedesco ha approvato il 22 giugno 2017 alcune modifiche al codice penale nazionale che consentirà, per i 38 reati penali previsti, l'installazione del software spia sui dispositivi mobili o fissi proprio per eludere la crittografia**.

L'ago della bilancia si è, dunque, spostato verso la Sicurezza nazionale piuttosto che sulla Privacy? Non proprio. I grandi *player* mondiali delle telecomunicazioni su Internet hanno fatto valere le proprie tesi a favore della nostra riservatezza, e probabilmente anche dei propri interessi economici, poiché il governo britannico ha fatto una piccola concessione: ha promesso che nessuna società sarà costretta a rimuovere la crittografia dei propri servizi **se non *tecnicamente fattibile*. Non ha tuttavia fornito una definizione di fattibilità tecnologica**. Sarà seguito dagli altri Stati anche su questa apertura?

Giovanni Nazzaro