The need for encryption grows

Con questo numero diamo inizio al 6° anno di "Sicurezza e Giustizia" con l'importante novità dell'adesione dell'*Europeans Telecommunications Standards Institut* (ETSI) ed, in particolare, di alcuni rappresentanti dei *Technical Committees* (TCs) per la *Lawful Interception* (LI) e la *Retained Data* (RD). **L'adesione segna un rilevante passaggio storico della rivista per l'oggettivo apprezzamento che giunge adesso anche oltre confine, sia per quanto attiene la scelta dei temi che tratta, sia per le modalità con cui li affronta**.
L'analisi delle nuove tecnologie nel contrasto al terrorismo attraversa ormai ogni settore ed ogni sua fase, persino quella della definizione degli *standards* di telecomunicazioni che saranno il riferimento per il futuro. In tale ambito è anche apprezzato il lavoro di formazione svolto dalla *Lawful Interception Academy*, alla sua seconda edizione, nel cui Report viene rilevato il ruolo dell'Italia come parte attiva nell'impegno internazionale nel contrasto al terrorismo. Un'Italia che, al contrario, è deficitaria per quanto attiene la sua presenza istituzionale sui tavoli europei, dove si discute degli *standards* sopra menzionati.

Oggi, l'impostazione classica nel contrasto agli eventi terroristici deve fare i conti, anche con nuove tecniche di comunicazione che utilizzano proprie modalità di trasmissione e di trattamento delle informazioni, in un mondo sempre più telematico ovvero basato su reti di nuova generazione. Non si tratta di tecnologie in quanto tali, quanto piuttosto di adattamenti di modalità di comunicazione esistenti, ma modificate secondo criteri proprietari. La differenza tra la nuova tecnologia di comunicazione e la nuova modalità di comunicazione è poco percepita in generale, ma è quello che fa la differenza oggi nelle indagini. Volendo semplificare, la tecnologia è lo "strumento" per comunicare, mentre la modalità di comunicazione è rappresentata dal "modo" con cui si usa lo strumento: per telefonare, per navigare su Internet, ecc. Un'indagine condotta nel moderno mondo delle telecomunicazioni non può prescindere in primo luogo dalla conoscenza delle tecnologie, in particolare delle regole tecniche e legislative che le governano, nonché delle metodologie standard per poterle supervisionare, in secondo luogo dalla conoscenza delle applicazioni utilizzate tramite le prime.

Molto si discute sull'utilizzo da parte dei terroristi di Skype, WhatsApp, Telegram. Queste applicazioni sono, però, solo alcune tra quelle che consentono di comunicare secondo modalità proprietarie, fino ad includere anche i giochi *online*, come è stato recentemente accennato dopo gli attentati di Parigi. Esistono, quindi, applicazioni che, qualora intercettate, non creerebbero problemi di comprensione circa le informazioni scambiate ed applicazioni che, invece, cifrano le comunicazioni che avvengono secondo regole, meglio protocolli, non conosciuti, rendendo il tutto quindi incomprensibile.

Quali che siano le modalità utilizzate per comunicare, tutte hanno in comune lo strumento che conserva tracce digitali: pensiamo al computer o al cellulare ormai sempre con noi. L'attenzione si sposta verso un problema di più semplice gestione solo apparentemente. Infatti, se in generale si può affermare che la tecnologia è governata da regole comuni quantomeno per consentirne l'interoperabilità, non si può escludere l'eccezione.
L'iPhone della Apple può essere un buon esempio di connubio tra nuova tecnologia e modalità proprietaria di comunicare. È recente la controversia tra Apple e l'FBI per sbloccare l'iPhone del terrorista della strage di San Bernardino, avvenuta il 2 dicembre 2015 all'Inland Regional Center, conclusasi con il successo dell'attività condotta in autonomia dall'FBI senza l'aiuto di Apple, che si era rifiutata di creare un software che potesse sbloccare qualunque iPhone. A livello mondiale ci sono state posizioni contrapposte a favore dell'una e dell'altra parte. Tra queste merita di essere richiamata quella di Adi Shamir, professore israeliano che ha contribuito alla creazione dell'algoritmo di crittografia RSA. Durante l'RSA Conference 2016, Shamir ha consigliato alla Apple di collaborare, così come aveva dimostrato in altre occasioni, ed attendere un banco di prova che fosse meno a favore dell'FBI. Nel caso specifico, ha evidenziato Shamir, si tratta di un caso nel quale sono morte 14 persone e si conosce il colpevole.

D'altra parte, in questi casi occorrerebbe distinguere con responsabilità. La discussione sulla creazione di una tecnologia per il controllo di massa, seppur legittimato, richiede tempi non paragonabili all'esigenza di ricerca della prova nell'immediatezza di un fatto criminoso. Inoltre, la storia insegna che questo tipo di approccio ha avuto sempre un epilogo negativo. Ricordiamo il "Chip Clipper" sviluppato dalla NSA che avrebbe dovuto essere adottato dalle compagnie telefoniche per cifrare le comunicazioni, annunciato nel 1993 e dismesso nel 1996, e lo studio "*Risks of Wiretap Modifications to Endpoints*" del 2013 pubblicato da 19 esperti mondiali di comunicazioni, cifratura e intercettazioni circa i rischi derivanti dalle modifiche che si vorrebbero introdurre nel CALEA Act, nel quale si afferma che creare *software* con *backdoor* potrebbe rendere più facile il lavoro dei cybercriminali.

È indubbio che i casi mediatici e l'onda emotiva possano aiutare a cambiare lo stato delle cose, ma il timore che le nostre comunicazioni siano intercettabili, anche da chi non ne abbia alcun diritto, costituirà il nuovo terreno di discussione che frappone esigenza di privacy e di indagine, senza dimenticare quella di *business* delle *big companies*. ©

Giovanni Nazzaro