Intercettazioni e tecnologia, i pericoli da evitare - Intervento di Antonello Soro

Intercettazioni e tecnologia, i pericoli da evitare

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali
("Il Messaggero", 24 maggio 2019)

I recenti sviluppi del "caso Exodus" ripropongono, sotto aspetti diversi, il tema delle intercettazioni. La notizia dell'accesso agli atti di centinaia di inchieste e dell'intercettazione di altrettanti cittadini del tutto estranei ad indagini dimostra il grado di pericolosità di strumenti investigativi fondati, come nel caso dei trojan, su tecnologie particolarmente invasive. Per un verso, infatti, i software utilizzati a questi fini presentano un'intrinseca pericolosità, potendo "concentrare", in un unico atto, una pluralità di strumenti investigativi, in alcuni casi non lasciando tracce o alterando i dati acquisiti. Si realizza, così una sorveglianza ubiquitaria, ogniqualvolta tali captatori siano installati su dispositivi mobili, che ci accompagnano in ogni momento della vita.

Per le loro stesse caratteristiche, dunque, i trojan, sfuggendo alle tradizionali categorie gius-processuali, rischiano di eludere le garanzie essenziali sottese al regime di acquisizione probatoria nei sistemi accusatori. Peraltro, se la prova decisiva risulta viziata, successivamente alla sua acquisizione, l'intero risultato processuale che su essa si fondi rischia di esseme travolto. Ulteriore elemento di criticità è, per altro verso, l'estemalizzazione di queste operazioni investigative, dovuta al loro elevato tasso di "tecnologizzazione". Ciò rende, infatti, assai più permeabile la filiera su cui si snoda l'attività di indagine, coinvolgendovi una pluralità di soggetti e spesso privi dei requisiti professionali, organizzativi e persino dell'affidabilità, necessari per svolgere un'attività così delicata quale quella intercettativa. Così anche il più rigoroso rispetto, da parte degli uffici giudiziari, delle misure di sicurezza da noi indicate a tutela della riservatezza dei dati intercettati rischia di essere del tutto vanificato dall'affidamento delle operazioni captative a società inadeguate e la cui compliance non è sempre agevole verificare, vista la molteplicità di soggetti a cui ciascuna Procura ha il potere di rivolgersi.

La frammentazione del processo investigativo e la delega di suoi segmenti importanti a privati ne accresce inevitabilmente le vulnerabilità, con danni spesso irreparabili non solo per la vita privata dei cittadini, ma anche per la stessa efficacia dell'azione investigativa. Casi come quelli di Exodus e, prima, Hacking Team dimostrano come carenze (colpose o, peggio, dolose) nelle misure di sicurezza a tutela dei dati rischino di trasformare il mezzo intercettativo - in sé prezioso - in un pericoloso strumento di dossieraggio massivo. Soprattutto ove si utilizzino - come nel caso Exodus - software connessi ad app, come tali posti su piattaform e accessibili a tutti e non direttamente inoculati nel solo dispositivo dell'indagato.

Se rese disponibili sul mercato in assenza - dolosa o colposa - dei filtri necessari a limitarne l'acquisizione da parte dei terzi, queste app rischiano, infatti, di trasformarsi in pericolosissimi strumenti di spionaggio massivo. È dunque ineludibile - come abbiamo indicato, anche di recente, al legislatore - un intervento normativo che rafforzi le garanzie previste sul punto dalla (attualmente sospesa) riforma "Orlando", contrastando soprattutto i rischi connessi al coinvolgimento di soggetti diversi nella "catena" delle indagini. Su un terreno che incrocia il potere investigativo e quello, non meno forte, della tecnologia, le garanzie sono irrinunciabili: mai come in questo caso, infatti, costituiscono forma e sostanza della democrazia.