LA NUOVA BUSSOLA QUOTIDIANA
Direttore Riccardo Cascioli
FATTI PER LA VERITÀ

LO SCANDALO

Il dossieraggio mette a rischio la sicurezza nazionale

POLITICA 30_10_2024

Ruben Razzante

Una domanda che bisognerebbe farsi in queste ore è la seguente: ma se una delle mille società di investigazione privata di Milano è in grado di mettere in ginocchio il sistema di sicurezza di un intero Paese, violando archivi e trafugando dati privati di decine di

cariche pubbliche, che cosa potrebbero fare alcuni servizi segreti stranieri se si interessassero in modo particolare alle vicende italiane?

Il quesito è tutt'altro che ozioso, perché il colabrodo digitale che sta emergendo dalle rivelazioni di queste ore, a Milano e ora anche a Roma, sollecita interventi urgenti da parte delle istituzioni, chiamate a mettere al centro la protezione di un diritto fondamentale dei cittadini, la riservatezza, e la tutela della sicurezza nazionale, che è un principio cardine della tenuta della nostra democrazia.

Quello che sta emergendo dalle cronache quotidiane degli ultimi giorni è un sistema capillare di dossieraggio condotto in particolare da ex funzionari dello Stato che lavorano in società private e che, disinvoltamente, usano le cosiddette porte girevoli per sfruttare il loro patrimonio di conoscenze e competenze acquisite negli anni e compiere azioni illecite e contrarie all'ordine pubblico. In un Paese che vive di conflitti di interessi e di imbarazzanti incompatibilità, pratiche del genere passano inosservate ma fanno il male del Paese e continuano a renderlo insicuro e pericolosamente esposto a scandali come quello che stiamo vivendo in queste ore.

Non si tratta più di singoli episodi, ma di una rete diffusa di spionaggio digitale che può compromettere la sicurezza di interi settori, privati e pubblici, con possibili ripercussioni sulla tenuta democratica del Paese. Già qualche anno fa il Ministro per l'innovazione tecnologica e la transizione digitale del Governo Draghi, Vittorio Colao aveva denunciato i rischi di una sottovalutazione dell'importanza della sicurezza informatica ma le forze politiche non si sono attivate più di tanto per prevenire furti di dati e spionaggi massicci.

Dossier riservati, informazioni sensibili, e persino dati strategici di interesse nazionale sembrano alla portata di chiunque abbia gli strumenti e le competenze per forzare i nostri sistemi informatici. Queste informazioni, una volta acquisite, possono essere usate per finalità subdole e persino eversive, mettendo a rischio la sicurezza stessa del nostro Stato e la stabilità delle istituzioni democratiche.

Peraltro va fatta una precisazione. Non si tratta di un fulmine a ciel sereno, visto che ogni giorno l'Autorità garante per la protezione dei dati personali riceve segnalazioni di data breach, cioè di violazioni di dati personali. Il dossieraggio ha ovviamente un impatto più devastante perché tocca soggetti pubblici, istituzionali, centri nevralgici di potere, ma la vulnerabilità dei nostri sistemi è quotidianamente confermata da molteplici abusi ai danni dei singoli e delle istituzioni. Il Garante della privacy ha annunciato di aver creato una task force interdipartimentale che coinvolge i settori di

competenza per individuare prontamente le attività da intraprendere e le maggiori garanzie a protezione delle banche dati. Come ha osservato il Presidente, Pasquale Stanzione, occorre, tra le altre cose, definire misure di sicurezza, tecniche e organizzative, adeguate riguardo agli accessi da parte del personale autorizzato, ma anche al complesso delle operazioni svolge dagli incaricati della loro gestione e manutenzione. Inoltre vanno portate avanti le attività ispettive nei confronti di società di investigazione privata.

La rivendita di informazioni riservate è la spia di una intensa e continua attività di spionaggio e saccheggio di dati contenuti nelle banche dati pubbliche da parte di agenzie di investigazione privata, tenute a rispettare regole che evidentemente non sempre rispettano.

Ecco perché, non servono commissioni parlamentari d'inchiesta, come auspicato da qualcuno, né nuove leggi o nuove Authority, bensì una più puntuale applicazione delle normative che già ci sono, atti amministrativi illuminati e incisivi, maggiori investimenti e tanta prevenzione. È necessario, cioè, potenziare i nostri sistemi di sicurezza con tecnologie all'avanguardia e con strategie di difesa che riescano a prevenire i crimini digitali ancor prima che questi si realizzino. Un investimento strutturale nella cybersicurezza, con risorse dedicate alla formazione e all'aggiornamento continuo degli operatori, è un passo imprescindibile per difendere i nostri dati.

La cybersicurezza dev'essere percepita come una priorità, esattamente come la sicurezza fisica del territorio. Il quadro attuale richiede un'azione coesa da parte di tutte le forze politiche e istituzionali del Paese, volta a mettere al centro la protezione dei dati dei cittadini e degli archivi delle nostre istituzioni. Senza divisioni e senza bandiere politiche, perché l'emergenza è collettiva e non risparmia nessuno.