

DIRITTO E SICUREZZA NAZIONALE

L'articolo 7. La legge che lega ogni impresa cinese all'intelligence dello Stato

Dietro le controversie su Huawei e TikTok non c'è un'azienda: c'è un'architettura giuridica. Come funziona — e perché rende impossibile una due diligence simmetrica.

di Carmine Di Marino

Quando si discute della pericolosità di un fornitore tecnologico cinese, il vero oggetto del contendere non è quasi mai una singola azienda. È un articolo di legge. L'articolo 7 della National Intelligence Law del 2017 impone a ogni organizzazione e cittadino cinese di «sostenere, assistere e cooperare» con il lavoro dell'intelligence nazionale. Attorno a questa formula ruota buona parte del dibattito occidentale sulla sicurezza tecnologica; conviene quindi leggerla per ciò che dice, e per ciò che rende possibile.

Un potere reso visibile, non creato

La National Intelligence Law, approvata nel 2017 e integrata nel 2018, è il testo più discusso del corpus normativo cinese. L'art. 7 fissa il dovere di cooperazione; l'art. 14 attribuisce all'apparato il potere di richiederla; l'art. 17 consente, nei casi urgenti, la requisizione di strutture e apparati. Ne discende la dottrina secondo cui nessuna impresa cinese può opporre un legittimo rifiuto a una richiesta dell'intelligence — argomento centrale nelle controversie sul caso Huawei. È importante notare che la legge non ha creato un potere nuovo: ha reso visibile un potere già esistente, veicolato dai comitati di Partito interni alle imprese.

La securitizzazione come regola, non come eccezione

Questa disposizione non è un episodio isolato, ma il vertice di una dottrina. La «sicurezza nazionale complessiva» formulata da Xi Jinping nel 2014 salda sicurezza e sviluppo e riconduce le tecnologie critiche entro il perimetro della sicurezza dello Stato: se la sicurezza economica è il fondamento di quella politica, il possesso di tecnologie critiche diventa una funzione di sicurezza nazionale. Sul piano analitico è un esercizio di securitizzazione, nel senso della Scuola di Copenaghen: un attore politico trasforma una questione in minaccia esistenziale, sottraendola alla normale procedura. Con una differenza decisiva: quella teoria presuppone la temporaneità dell'eccezione, mentre nel caso cinese la securitizzazione è la regola, priva del momento di ritorno alla normalità.

Il giro di vite del 2023

La riforma della Counter-Espionage Law del 26 aprile 2023 illustra bene questo meccanismo. Il testo del 2014 definiva lo «spionaggio» con riferimento ai soli segreti di Stato; la riforma lo estende a «documenti, dati, materiali e oggetti attinenti alla sicurezza e agli interessi nazionali». Poiché la legge non definisce né «sicurezza» né «interessi nazionali», qualunque attività di raccolta — la mappatura di una filiera, il giornalismo d'inchiesta, la ricerca accademica, la due diligence in un'operazione di M&A — può essere ricondotta alla fattispecie a posteriori. Il perimetro del lecito non è conoscibile ex ante: è questa indeterminatezza, più della severità astratta della norma, a produrre l'effetto dissuasivo.

E i dati non escono

Il quadro si chiude con la Data Security Law, in vigore dal 2021, che protegge il dato non come proiezione della persona ma come risorsa strategica dello Stato. L'art. 21 ne istituisce una classificazione gerarchica, l'art. 2 ne afferma la portata extraterritoriale, e soprattutto l'art. 36 vieta ai soggetti situati in Cina di fornire dati ad autorità giudiziarie straniere senza previa approvazione delle autorità cinesi. Mobilitazione universale, proiezione extraterritoriale e controllo del flusso informativo sono le tre funzioni che l'impianto realizza in combinato disposto.

L'asimmetria che nessuna diligenza elimina

La conseguenza pratica, per chi opera dall'Europa, va enunciata senza eufemismi: l'acquirente o il partner europeo non può condurre sulla controparte cinese la stessa due diligence che questa può condurre su di lui. Non è un incidente, è un effetto di sistema, e nessuna diligenza professionale lo elimina. Il rischio va allora prezzato o strutturato: dichiarazioni e garanzie sui rapporti con l'apparato di sicurezza, meccanismi di escrow, clausole risolutive collegate all'inserimento in liste di misure restrittive, segregazione del patrimonio informativo. È il passaggio in cui una questione apparentemente geopolitica diventa una clausola contrattuale.

NOTA DI METODO

La distinzione dirimente è tra ciò che la legge dice e come viene applicata. Il testo dell'art. 7 è un fatto documentato; la sua portata effettiva — quanto spesso e con quale intensità la cooperazione sia realmente esatta — resta una valutazione, perché poggia su una prassi opaca e non verificabile dall'esterno. Trattare l'una per l'altra è l'errore più comune del dibattito pubblico.

Fonti principali

National Intelligence Law della RPC, 27 giugno 2017 (integrata nel 2018), artt. 7, 14, 17.

Counter-Espionage Law della RPC, 1º novembre 2014, come modificata il 26 aprile 2023.

Data Security Law della RPC, in vigore dal 1º settembre 2021, artt. 2, 21, 36.

National Security Law della RPC, 1º luglio 2015.

B. Buzan, O. Wæver, J. de Wilde, Security: A New Framework for Analysis, Lynne Rienner, 1998.