GERMANIA

Tribunale costituzionale federale, ordinanza dell'8 giugno 2021 (1 BvR 2771/18), sul dovere di tutela dello Stato in relazione alla vulnerabilità della sicurezza informatica (le cosiddette vulnerabilità *zero-day*)

23/07/2021

Il Tribunale costituzionale federale ha respinto un ricorso costituzionale riguardante lo sfruttamento da parte dello Stato delle vulnerabilità della sicurezza informatica che sono ancora sconosciute anche ai produttori di *software* e *hardware* (le cosiddette vulnerabilità *zero-day*). Il ricorso è stato ritenuto inammissibile perché, da un lato, i ricorrenti non avevano sufficientemente dimostrato la possibilità di una violazione del dovere costituzionale dello Stato di tutela contro l'accesso non autorizzato di terzi ai sistemi informatici e, dall'altro, il ricorso non soddisfaceva i requisiti di sussidiarietà in senso lato.

I ricorrenti contestavano una norma della legge sulla polizia del *Land* Baden-Württemberg (art. 54 PolG BW) che consente il monitoraggio segreto del contenuto delle telecomunicazioni a fini preventivi per proteggere alcuni importanti interessi giuridici. Secondo tale norma è tra l'altro possibile la cosiddetta sorveglianza delle telecomunicazioni alla fonte (*Quellen-TKÜ*), la quale richiede che il sistema di destinazione possa essere violato attraverso l'introduzione di un *software* di sorveglianza. Questo può essere fatto in diversi modi. Il ricorso si riferiva in particolare a quella tipologia di infiltrazione che sfrutta le vulnerabilità *zero-day* nell'*hardware* o nel *software* del sistema di destinazione. In sostanza, i ricorrenti sostenevano che, introducendo la facoltà della sorveglianza alla fonte, il *Land* Baden-Württemberg avesse violato la riservatezza e l'integrità dei sistemi informatici garantiti dai diritti fondamentali, perché le autorità non avrebbero più alcun interesse a segnalare ai produttori le vulnerabilità a loro note proprio perché potrebbero utilizzarle per infiltrarsi nei sistemi informatici per la sorveglianza delle telecomunicazioni alla fonte consentite in base alla normativa scrutinata. Senza una segnalazione al produttore, tuttavia, le vulnerabilità della sicurezza informatica e i pericoli a essa associati, quali ad esempio l'attacco da parte di terzi ai sistemi informatici, continuerebbero a persistere. Lo Stato, in base al suo dovere di tutela, avrebbe quindi dovuto introdurre una disciplina di accompagnamento per la gestione delle vulnerabilità, che in particolare vietasse l'uso delle vulnerabilità di sicurezza che non fossero note al produttore del sistema in questione. Anche senza considerare lo sfruttamento delle lacune *zero-day* di per sé incompatibile con il dovere di tutela dello Stato, si sarebbe dovuto comunque prevedere una procedura amministrativa per la valutazione delle lacune di sicurezza informatica nei singoli casi.

Il *Bundesverfassungsgericht* ha affermato in linea di principio la sussistenza di un dovere di tutela dello Stato e la responsabilità di quest'ultimo per la protezione dei diritti fondamentali,

garantendo la sicurezza dei sistemi informatici (nella specie, sono stati ritenuti interessati la segretezza delle telecomunicazioni e la garanzia della riservatezza e dell'integrità dei sistemi informatici). Lo Stato deve infatti contribuire alla protezione degli utenti dei sistemi informatici contro gli attacchi subiti da terzi. Tuttavia, i ricorrenti non avevano dimostrato nel modo richiesto che tale dovere di protezione sarebbe stato violato. Il Tribunale ha inoltre ricordato che l'introduzione e l'implementazione normativa di un concetto di protezione spetta al legislatore, che in linea di principio ha un proprio margine di valutazione e di progettazione sotto questo profilo.

Maria Theresia Roerig