07-APR-2022
da pag. 15 / foglio 1 / 2

Il Sole 24 ORE
Dir. Resp.: Fabio Tamburini
Tiratura: 81177 Diffusione: 137712 Lettori: 756000 (0001998)

Sicurezza, settori strategici e banda larga: come cambia la protezione dei dati

Convivere col cybermondo / 1

Michele Colajanni, Giusella Finocchiaro, Stefano Mele e Oreste Pollicino

La guerra in Ucraina ha ridisegnato i modelli di sovranità, anche digitale, e ha costretto gli Stati a ridefinire il perimetro della sicurezza nazionale, ovviamente anche con uno specifico focus alle minacce provenienti dal cyberspazio. Gli Stati e le organizzazioni sovranazionali sono stati bruscamente ricondotti a una riconfigurazione della propria strategia difensiva nella quale oggi gioca un ruolo strategico e irrinunciabile la cybersecurity.

Anche il Governo italiano si è mosso in questa direzione, con il recentissimo decreto legge n. 21 del 21 marzo 2022, che prevede alcune misure urgenti per contrastare gli effetti economici e umanitari della crisi in Ucraina. Tra le numerose azioni previste, il legislatore si è concentrato su un ulteriore rafforzamento dei presidi per la sicurezza, la difesa nazionale e per le reti di comunicazione elettronica, nonché sulla revisione della normativa in materia di "Golden Power".

Il legislatore ha infatti previsto una riorganizzazione complessiva dei poteri speciali in materia di comunicazione elettronica a banda larga basati sulla tecnologia 5G, riscrivendo completamente e ampliando il contenuto dell'articolo 1-bis del decreto-legge n. 21 del 15 marzo 2012.

In questo specifico settore, infatti, il nuovo decreto legge, da un lato, conferma come attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, dall'altro – ed è qui la prima importante novità – apre anche a tutti gli ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud, che saranno individuati, di concerto con gli altri Ministri competenti, con uno o più decreti successivi del Presidente del Consiglio dei ministri. Dunque si estende, potenzialmente, l'ambito dei servizi digitali strategici, per il momento definiti con una formula generale che dovrà essere oggetto di successiva specificazione (come si è detto sopra: «servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud»). Un perimetro già ampio e destinato ad estendersi ulteriormente.

La novità normativa è di grande impatto: richiede che le imprese, prima di procedere all'acquisizione, a qualsiasi titolo, anche attraverso contratti o accordi, di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di rilevanza strategica, ovvero componenti ad alta intensità tecnologica funzionali alla realizzazione o gestione di attività di rilevanza strategica, notifichino alla Presidenza del Consiglio dei ministri un articolato e complesso "piano annuale", il cui contenuto è minuziosamente dettagliato nel decreto legge e comporta, tra gli altri, anche l'obbligo di specificare la lista dei fornitori attuali e potenziali.

Ricevuto il piano annuale, inoltre, la Presidenza del Consiglio dei ministri (i) approva entro trenta giorni dalla notifica, prorogabili per due volte di altri venti giorni, laddove sia necessario svolgere approfondimenti riguardanti aspetti tecnici, oppure (ii) impone specifiche prescrizioni o condizioni, ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale, o ancora (iii) approva, in tutto o in parte, il piano per un periodo temporale, anche limitato, indicando un termine per l'eventuale sostituzione di determinati beni o servizi, o infine (iv) esercita il potere di veto. Il mancato rispetto delle prescrizioni impartite dalla Presidenza del Consiglio dei ministri in fase di verifica del piano annuale comporta anche l'attivazione di un complesso sistema sanzionatorio, che, in caso di omissione della notifica o di mancata osservanza delle prescrizioni, comporta l'applicazione di sanzioni amministrative che possono arrivare fino al 3% del fatturato dell'impresa.

Inoltre, sono considerati nulli i contratti o gli accordi compresi nella notifica se eseguiti prima che sia decorso il termine per l'approvazione del piano o in violazione dello stesso. In tali casi, il Governo può ingiungere all'impresa di ripristinare a sue spese la situazione anteriore all'esecuzione, stabilendo il relativo termine, con l'applicazione di ulteriori sanzioni amministrative in caso di ritardi.

Inoltre, un'ulteriore novità di rilievo è costituita dall'introduzione di un sistema di monitoraggio finalizzato a controllare l'osservanza delle prescrizioni e delle condizioni impartite dal Governo nell'esercizio dei poteri speciali, a verificare la loro adeguatezza e ad appurare l'adozione delle misure attuative, anche tecnologiche, imposte. Le attività di monitoraggio sono svolte da uno specifico comitato composto da uno o più rappresentanti della Presidenza del Consiglio dei ministri e dei Ministeri rilevanti, oltre dall'Agenzia per la cybersicurezza nazionale, oltre che, se ritenuto necessario, del Centro di valutazione e certificazione nazionale (CVCN) e delle articolazioni tecniche dei Ministeri dell'interno e della difesa. Peraltro, per agevolare le attività di monitoraggio, le imprese dovranno comunicare – con la periodicità indicata con il provvedimento di

Il Sole 24 ORE
Dir. Resp.: Fabio Tamburini
Tiratura: 81177 Diffusione: 137712 Lettori: 756000 (0001998)

esercizio dei poteri speciali – ogni attività esecutiva posta in essere, fornendo i dettagli tecnici ed evidenziando le ragioni idonee ad assicurare la conformità al piano, nonché inviare una relazione periodica semestrale sulle attività eseguite.

Infine, il comitato di monitoraggio dispone della facoltà di svolgere ispezioni e verifiche tecniche, relativamente ai beni e alle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione dei servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché ad altri possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi, oggetto del provvedimento di esercizio dei poteri speciali.

Difendersi, anche dagli attacchi digitali, è necessario. Occorre, però, che il Paese possa continuare a correre, cercando di mantenere viva quella ripresa che, prima della guerra, avevamo intravisto. Le nuove disposizioni, dunque, non dovranno rappresentare nuovi oneri e nuovi ostacoli per le imprese e per la pubblica amministrazione che stanno cercando di ripartire e di fare un salto, anche in ambito digitale, con la leva costituita dal Pnrr.

Conciliare necessità di difesa e esigenze di semplificazione rappresenta, indubbiamente, un'ulteriore inevitabile sfida.

Michele Colajanni, Professore di Ingegneria informatica, Università di Bologna
Giusella Finocchiaro, Professoressa di Diritto di Internet, Università di Bologna e Co-founder DigitalMediaLaws
Stefano Mele, Partner, Gianni & Origoni
Oreste Pollicino, Professore di Internet Law, Università Bocconi e Co-founder, DigitalMediaLaws