Cybersecurity nel settore energetico: scenario, indirizzi normativi e compliance per le imprese

Svenja Bartels e Giuliana Viviano, Avvocati - Studio Rödl & Partner

La carica innovativa portata dalla digitalizzazione e dall'applicazione nei processi aziendali delle tecnologie 4.0, quali l'Internet of Things ("IoT"), la Blockchain e l'intelligenza artificiale, ha un impatto significativo anche in un contesto complesso quale quello energy e delle utilities. Si considerino, ad esempio, le nuove "smart grids" che trasmettono dati, in tempo reale, dai contatori e dagli altri strumenti connessi agli utenti, per poi razionalizzare e distribuire l'energia in maniera efficiente e decentrata, o gli "smart meter" (i c.d. contatori intelligenti) che, combinati con l'uso della blockchain, forniscono all'utente certificazioni trasparenti sull'entità dei consumi.

La digitalizzazione, con la conseguente raccolta e trasporto dell'enorme quantitativo di dati che inevitabilmente comporta, ha determinato tuttavia l'insorgere anche di nuovi rischi. In particolare, tali tecnologie possono trovarsi esposte a cyber attacchi e incidenti informatici tali da poter compromettere irrimediabilmente la business continuity delle imprese e, più in generale, la stessa sicurezza energetica nazionale ed europea. Le reti elettriche e i gasdotti sono del resto fortemente interconnessi in tutta l'UE (… e anche oltre), con il risultato che un incidente cyber in uno dei nodi della rete può provocare, con un vero e proprio effetto a cascata, blackout o carenze di approvvigionamento energetico nei vari Stati Membri.

In questo scenario, è chiaro, quindi, che la cybersecurity non possa essere più trascurata dagli operatori del settore energy, tanto più che il legislatore sia europeo, sia italiano considerano oramai il settore energy e la cybersecurity in un rapporto di stretta continuità tale per cui la trasformazione digitale del primo non può prescindere dall'adozione di adeguate misure per il la seconda.

A tale riguardo, nel contesto prettamente italiano, si rammenta anzitutto il decreto-legge n.105/2019 – convertito con la recente legge del 18 novembre 2019, n. 133 - che ha ufficialmente istituito il c.d. "perimetro di sicurezza nazionale cibernetica", perimetro di cui faranno parte le amministrazioni pubbliche, gli enti e gli operatori nazionali (anche privati), in presenza di alcuni specifici requisiti, tra cui l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato.

Tra tali soggetti, verosimilmente, ricadono anche i maggiori operatori del settore energy, sebbene oggi si sia ancora in attesa del decreto del Presidente del Consiglio dei ministri, atto ad individuare i soggetti effettivamente rientranti nel suddetto perimetro. Da notare in ogni caso che il provvedimento in parola ha introdotto anche nuove fattispecie rilevanti in materia di responsabilità amministrativa degli enti di cui al D. lgs 231/2001. Ciò, sanzionando i soggetti che, allo scopo di ostacolare o condizionare gli adempimenti derivanti dall'appartenenza al perimetro di sicurezza, forniscono informazioni, dati o elementi di fatto non rispondenti al vero, necessari per la predisposizione delle comunicazioni o per l'aggiornamento degli elenchi delle reti, dei sistemi informatici, ovvero non forniscano i predetti dati entro i termini legislativi previsti.

Si ricordano, inoltre, nell'ambito regolamentare europeo, la direttiva NIS n.2016/1148 – recepita in Italia dal D. Lgs. n. 65/2018 – e, soprattutto, il Regolamento UE n. 881/2019 (il c.d. "Cybersecurity Act").

La direttiva NIS impone agli Operatori di Servizi Essenziali - fra cui sono ricompresi i soggetti, pubblici o privati, che forniscono servizi essenziali nel settore dell'energia - l'adempimento di taluni stringenti obblighi, tra i quali:

- L'adozione di misure tecniche e organizzative adeguate alla gestione dei rischi ed alla prevenzione e minimizzazione dell'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi;
- nonché la notifica, senza ritardo, degli incidenti che abbiano un impatto rilevante sulla continuità del servizio, al Computer Security Incident Response Team di ogni Stato Membro.

Il Cybersecurity Act, dall'altro lato, prevede la realizzazione di schemi di certificazione specifici per i dispositivi connessi che, una volta predisposti dall'ENISA (l'European Union Agency For Cybersecurity) e adottati poi dalla Commissione Europea, potranno essere richiesti dalle imprese, ragione-

volmente, anche con riferimento agli "smart meter".

A completamento del quadro sopra descritto, si segnala infine la Raccomandazione n. 553 del 3 aprile 2019 sulla cybersecurity nel settore dell'energia che non è, invero, vincolante né per gli Stati membri, né per gli operatori del settore, ma nondimeno è utile per identificare le questioni di cybersecurity ritenute più urgenti e le relative misure consigliate. In sintesi, la Raccomandazione individua tre tipi di misure:
a) le misure connesse alle esigenze delle componenti dell'infrastruttura energetica operanti in tempo reale per cui i gestori delle reti elettriche dovrebbero applicare le più recenti norme tecniche di sicurezza;
b) le misure volte a prevenire "effetti a cascata", per cui i gestori delle reti elettriche dovrebbero tener conto degli "effetti cyberfisici" al momento della definizione dei piani di continuità operativa e assicurare che i nuovi dispositivi intelligenti mantengano un livello di cybersecurity adeguato alla criticità del caso; e infine
c) le misure volte a far coesistere le tecnologie preesistenti e tecnologie all'avanguardia nel settore energetico, per cui i gestori delle reti elettriche dovrebbero aggiornare alla versione più recente il software e l'hardware dei sistemi preesistenti, ed effettuare un'analisi dei rischi cyber per connettere questi impianti con i nuovi.

A fronte del complesso quadro regolatorio sopra descritto, si osserva tuttavia che l'elaborazione normativa non è ancora giunta a enucleare al massimo livello di dettaglio le misure di cybersecurity dirette agli operatori del settore energy, stante il complesso processo di implementazione della normativa di attuazione con riferimento, in particolare, alla Direttiva NIS, e al c.d. Perimetro di sicurezza Nazionale.

Tale circostanza, tuttavia, non esime le imprese dal sottovalutare il rischio di cyber attacchi.

Per le imprese, rimane infatti prioritario porre in essere progetti di risk management integrato che, partendo dalla mappatura dei rischi rilevanti, non solo in relazione ai rischi sanzionatori, ma anche più in generale in tema di rischi di perdita di dati e di danno al proprio patrimonio aziendale, indichino gli interventi di remediation, le policy e le misure tecniche e organizzative idonee a prevenire, gestire e mitigare tali rischi. Ciò, appunto, in primis al fine di evitare attacchi o incidenti tali da determinare la perdita della business continuity ed un inevitabile danno alla reputazione.

L'auspicio, in conclusione, è che le imprese in generale, ed anche quelle che operano nel settore energy, che stanno sviluppando nuovi modelli di business nel nuovo contesto digitale e delle nuove tecnologie, pongano l'attenzione sulla pericolosità dei rischi cyber e si convincano, quindi, dell'ineluttabilità di adottare Modelli Organizzativi Integrati per la gestione dei predetti rischi e la compliance alle normative succitate.