Maria Cristina Cataudella

Tavola rotonda: "*La gestione del rischio nelle infrastrutture critiche: tra norme e compliance*". Brevi spunti di riflessione.

a) La definizione nella normativa europea e nazionale di "*infrastrutture critiche*"

Un primo spunto di riflessione che vorrei suggerire ai partecipanti a questa tavola rotonda, riguarda proprio la definizione di "*infrastrutture critiche*".

In una prima approssimazione possiamo definire "critiche" quella infrastrutture da cui dipende lo sviluppo, la sicurezza e la qualità della vita nei Paesi industrializzati. E' chiaro che si tratta di una definizione molto ampia che richiede di essere puntualizzata e affinata per delimitare con chiarezza i confini tra "infrastruttura critica" e "infrastruttura non critica", in particolare ai fini dell'individuazione dei soggetti che sono destinatari di alcuni precisi obblighi in materia di sicurezza.

Come emerge, tuttavia, dalla normativa sia europea che nazionale che si prenderà in considerazione, destinatarie delle disposizioni in materia di sicurezza sono solo in alcuni casi le "*infrastrutture critiche*" (direttiva 2008/114/CE), in altri casi, invece, sono soggetti che non coincidono pienamente con le infrastrutture critiche, come gli "*operatori di servizi essenziali*" (direttiva 2016/1148/UE) o come "*le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati… inclusi nel perimetro di sicurezza nazionale cibernetica*" (d.l. n. 105 del 2019).

Una prima definizione normativa di infrastruttura critica la troviamo nella direttiva 2008/114/CE *"relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione"*. Il punto a) dell'art. 2 della cit. direttiva definisce infrastruttura critica "*un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni*".

Se è vero che la direttiva del 2008 contiene una definizione generale di "*infrastruttura critica*", bisogna però puntualizzare che si tratta di una definizione, da una parte, funzionale, perché volta all'individuazione delle "*infrastrutture critiche europee*"[1] (ECI) e, dall'altra parte, parziale, perché la direttiva non si applica a tutte le infrastrutture critiche ma solo a quelle che operano nei settori dell'elettricità e dei trasporti.

Successivamente la c.d. direttiva NIS (2016/1148/UE), finalizzata a incrementare la preparazione e la cooperazione degli Stati membri nell'ambito della sicurezza informatica, sostituisce alla definizione di "*infrastrutture critiche*" quella di "*operatori di servizi essenziali*"[2]. Non c'è perfetta coincidenza tra le due definizioni: la definizione di operatori di servizi essenziali è infatti più ampia ed ha una focalizzazione ancora più forte sul concetto di servizio. Si deve, tuttavia, rilevare che, se da una parte, la direttiva NIS si applica anche ad entità diverse rispetto alle solo infrastrutture critiche, dall'altra parte, rispetto alla direttiva del 2008, è limitata al solo ambito della sicurezza informatica.

Passando alla normativa nazionale, si deve rilevare come il recentissimo d.l. n. 105 del 2019 ("*Disposizioni urgenti in materia di perimetro di sicurezza cibernetica nazionale*"), prevede degli obblighi - sempre in materia di sicurezza informatica - per "*le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati… inclusi nel perimetro di sicurezza nazionale cibernetica*", ovvero quelli che saranno individuati in base ai due criteri dettati dal d.l. n. 105 del 2019 stesso: "*il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato*" e "*l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale*". Anche in questo caso abbiamo, pertanto, una definizione dei soggetti che devono adempiere agli obblighi di sicurezza che, pur avvicinandosi, non coincide perfettamente con quella delle due normative europee sopra citate. In particolare, in questo caso, insieme a chi presta un servizio essenziale, viene preso in considerazione anche chi svolge una funzione essenziale.

---

[1] L'"infrastruttura critica europea" viene invece definita come "*un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture*".

[2] Ai sensi dell'art. 5, i criteri per identificare gli operatori di servizi essenziali sono i seguenti: "*a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; e c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio*".

b) Sicurezza delle infrastrutture critiche e protezione della riservatezza

Un altro aspetto sul quale vorrei focalizzare l'attenzione è quello della conciliazione tra diritto alla riservatezza e alla protezione dei propri dati personali (che trovano un forte riconoscimento proprio nel regolamento 2016/679 c.d. GDPR) e la difesa della sicurezza delle infrastrutture critiche (direttiva 2008/114CE; direttiva 2016/1148UE). In alcuni casi, infatti, la difesa della sicurezza delle infrastrutture critiche potrebbe richiedere dei sacrifici in termini di protezione della riservatezza e dei dati personali. Basti pensare alle misure predisposte in caso di rischi di attentati terroristici, che prevedono, in alcuni casi, il controllo a tappeto su conversazioni telefoniche, messaggi, e mail, siti web che vengono visitati o dati personali.

La domanda allora è: fino a che punto la riservatezza delle persone e la protezione dei loro dati personali può essere compressa per ragioni di sicurezza nazionale?