ALCUNE RIFLESSIONI SULLA DATA PROTECTION E LE INFRASTRUTTURE CRITICHE NAZIONALI.

La nuova economia digitale sta ponendo con prepotenza ai Governi europei e ed extra europei il tema della data protection e quello del rispetto della privacy come diritto fondamentale della persona.

Rimanendo nell'alveo del nostro continente è stato da ultimo varato il recente pacchetto protezione dei dati composto dal Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini.

Inoltre il Parlamento Europeo ha adottato il 6 luglio del 2016 la Direttiva sulla sicurezza dei sistemi delle reati e dell'informazione (Network and Information Security), detta anche Direttiva NIS. Quest'ultima rappresenta il primo insieme univoco di regole sulla sicurezza informatica a livello dell'Unione Europea con l'obiettivo di raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti i Paesi membri dell'UE. Difatti come più volte sostenuto dal Garante Europeo la *cybersicurezza* è «un problema vitale e strategico per una democrazia moderna», che non deve fermarsi a una riga di bilancio.

Il trattamento, la riservatezza e la protezione dei dati personali, sensibili, particolari o comunque "critici" per le infrastrutture nazionali presenta rischi elevati e specifici. "Il fenomeno dei social network e la geolocalizzazione dei terminali impone nuove metriche e strumenti per proteggere ambienti e asset tangibili e virtuali".

Ai sensi della Direttiva gli Stati membri dovrebbero essere competenti per determinare quali soggetti soddisfino i criteri stabiliti nella definizione di operatore di servizi essenziali e in seguito al processo di identificazione, dovrebbero adottare misure nazionali dirette a determinare i soggetti cui si applicano gli obblighi in materia di sicurezza delle reti e dei sistemi informativi.

Per fornire una indicazione dell'importanza in relazione al settore interessato gli Stati dovrebbero tener conto del numero e delle dimensioni degli operatori identificati, ad esempio in termini di quota di mercato anche al fine di valutare se un incidente avrebbe effetti negativi su di un servizio essenziale.

"Cosa significhi colpire una infrastruttura critica collegata alla gestione di quantità massive di dati, per esempio i dati personali dei cittadini, è intuibile osservando alcuni fra gli attacchi più noti operanti nel territorio cibernetico degli ultimi anni. Relativamente all'attacco alla Sony del 2011 furono rubati dati, tra cui credenziali per carte l'uso di carte di credito, di oltre cento milioni di clienti."

Il tema della protezione del cyberspazio è stato rappresentato in tutta la sua gravità dal Generale Claudio Graziano, Capo di Stato Maggiore della Difesa il quale ha dichiarato: "*Oggi il campo di battaglia più importante è il cyberspazio: la capacità di proteggere e attaccare le reti di computer*", e ancora *"non avevamo compreso la dimensione della minaccia, ma ci stiamo attrezzando. Abbiamo creato il Cioc, Comando interforze operazioni cibernetiche, che è già in funzione e dal 2018 sarà a pieno regime."*

Tale principio vale con particolare riguardo alla tutela delle infrastrutture critiche nazionali, siano esse pubbliche che gestite da operatori privati. A tale riguardo si renderà necessario sempre più porre un focus in relazione al settore privato, posto che come già rappresentato nelle predetta Direttiva NIS, al considerando 35, la maggioranza delle reti e dei sistemi informativi è gestita da privati e che la collaborazione tra il settore pubblico e il settore privato è essenziale.

I Governi nazionali dovranno pertanto completare al più presto il progetto già avviato di identificazione delle predette infrastrutture, e normare i requisiti minimi di protezione, in linea con l'impostazione attuale della gestione della sicurezza come strumento di mitigazione del rischio, nel rispetto dei vincoli di interdipendenza che i sistemi complessi nei quali siamo immersi determinano.

Potrebbe inoltre rendersi necessario riconsiderare alcuni capisaldi del liberismo economico che in prospettiva sembrano poter cozzare con i basilari principi di sicurezza dello spazio europeo e/o nazionale, per porsi un interrogativo in merito al necessario ruolo della vigilanza e/o partecipazione Statale nei settori strategici nonché essenziali del sistema Paese.

I trattamenti in cloud computing, la delocalizzazione di server, la possibilità di accedere da remoto da paesi terzi spesso portatori di culture diverse e antitetiche a quelle democratiche del nostro continente, non dovrebbero essere lasciate esclusivamente in balia delle seppur stringenti sole regole contrattuali previste dalla commissione Europea. Uno scenario preoccupante, che diviene ancor più inquietante nell'era che si affaccia: quella dell'Internet delle cose.

La rivoluzione dei Big data stravolgerà il mondo e proteggere il proprio sistema sociale è dovrebbe essere un obiettivo chiaro nella declinazione di ogni strategia nazionale, pertanto in tema di infrastrutture critiche, si renderà sempre più necessario fare fronte agli aspetti legati alla sicurezza, con particolare attenzione all'ambito dell'anti terrorismo.

Ada Fiaschi