# DATA PROTECTION NEL MEDIO ORIENTE

**L'aumento nella produzione legislativa in tema di protezione dei dati personali e la consapevolezza, dei settori pubblici e privati, sull'importanza della condivisione delle informazioni e della relativa titolarità, creano nuove sfide ed opportunità che impatteranno consumatori ed aziende a livello globale. Oggigiorno, i dati sono considerati un *asset* strategico e una potente risorsa con valore economico. Per proteggere la *privacy* dei clienti e per creare e sviluppare nuovi modelli per la gestione integrata delle informazioni, le aziende ed i governi necessitano appropriate metodologie per organizzare e proteggere i dati personali ed essere in linea con i requisiti imposti dalle regolamentazioni in materia. L'uso errato o la mancata gestione di questi ultimi potrebbe influenzare negativamente la percezione pubblica dell'organizzazione stessa nel mercato; nel senso opposto, una società potrebbe guadagnare vantaggi competitivi e fiducia da parte dei clienti attraverso la corretta applicazione dei principi di *"data protection by design"*.**

**Massimo PAPA,** Professore ordinario di Diritto Musulmano e dei Paesi Islamici, Facoltà di Giurisprudenza, Università di Roma Tor vergata.

**Gabriele DONADEI,** Sottotenente Ufficiale, frequentatore della Scuola Ufficiali dell'Arma dei Carabinieri di Roma.

## 1. L'importanza della protezione dei dati nei paesi mediorientali

I Paesi del Consiglio di Cooperazione del Golfo (GCC)[1] sono i protagonisti di un massivo sviluppo economico e tecnologico, che porterà grandi innovazioni negli assetti urbani nei prossimi dieci o vent'anni. Gli Emirati Arabi Uniti (UAE) sono sicuramente i pionieri di queste grandi ambizioni, ma Qatar, Bahrain e Oman, grazie alle loro ingenti capacità economiche, potranno, presto, soddisfare le esigenze di un mondo in continuo cambiamento. L'intera area sta adottando nuove normative in tema di protezione dei dati, consolidando regolamenti già esistenti o espandendone il raggio d'azione, con l'obiettivo di difendere i diritti dei singoli cittadini, di costruire nuove tecnologie ed incrementare il flusso di dati internazionale e regionale. Il settore *data protection* è trainante tra i governi del Medio Oriente, che stanno investendo considerevolmente in automazione, *smart cities* ed innovazione scientifica.

## 2. Uno sguardo sulle principali legislazioni

Il Qatar è stato il primo Paese del GCC ad approvare ed emanare una legge nazionale sulla protezione dei dati personali; con la legge n.13/2016 "*Concerning Personal Data Protection*" (DPL) il governo qatariota ha voluto assicurare uno standard minimo di protezione dei dati, diritti per gli utenti e linee guida per le organizzazioni per il trattamento dei dati personali all'interno del Qatar. È necessario evidenziare, però, che la legge, non regolando la normativa nel dettaglio, ha necessitato di un'integrazione, da parte del *Compliance and Data Protection Department*, attraverso 14 linee guida specifiche. La previsione legislativa, di 31 articoli, individuando il Ministero dei Trasporti e della Comunicazione come ente regolatore e garante, trova la sua applicazione in ogni dato che sia processato, raccolto o estratto elettronicamente od ottenuto a seguito di un processo risultante da metodologie tradizionali ed elettroniche. La legge prevede che ogni organizzazione che processi dati personali debba aderire ai principi di trasparenza, chiarezza e rispetto della dignità umana, nonché ottenere, in ottemperanza alla previsione dell'art. 4, l'espresso consenso del soggetto titolare del dato; ciononostante, lo stesso articolo 4 permette la raccolta, senza autorizzazione, di tutte quelle informazioni necessarie per fini legali. Con riferimento ai requisiti di notifica a seguito di una violazione dei sistemi di protezione dei dati, gli articoli 13 e 14 del DPL fanno espresso riferimento a quelle infrazioni che "*cause serious damage*" ai dati personali e alla *privacy* dell'individuo, necessitando la comunicazione, da parte dell'organizzazione, all'ente regolatore, il quale sarà il responsabile di successivi avvisi al soggetto interessato e al *Compliance and Data Protection Department*. È da notare che il DPL non fa alcun riferimento alla finestra temporale per effettuare la notifica; tale vuoto normativo, però, è stato integrato dalle linee guida che prevedono una *deadline* di 72 ore dal momento in cui la violazione è stata rilevata. È necessario sottolineare, in questa sede, che in occasione dell'organizzazione della Coppa del Mondo FIFA 2022, tenutasi in Qatar nel dicembre 2022, il governo qatariota ha installato circa 15 mila telecamere negli 8 stadi che hanno ospitato la competizione calcistica. Il sistema di videosorveglianza, attivo 24 ore su 24 e gestito interamente all'interno dell'*Aspire Control and Command Center*, ha posto una serie di interrogativi riguardo il rispetto dei principi di tutela della *privacy*. Il sistema, in grado di osservare contemporaneamente tutti gli stadi, ha permesso il controllo da remoto dell'evento; dall'*Aspire Center*, gli organizzatori potevano aprire e chiudere i cancelli, per gestire il flusso dei tifosi, analizzare gli indicatori di temperatura e umidità, per prevedere eventuali assembramenti pericolosi, nonché effettuare un conteggio effettivo dei visitatori, non più sulla base dei biglietti venduti ma sull'effettiva presenza. La vera novità, però, è rappresentata dal "*digital twin*", una tecnologia che ha permesso la riproduzione dello stadio in una realtà virtuale, dove viene riprodotto interamente ciò che succede all'interno dell'impianto sportivo e durante l'evento calcistico.

Negli Emirati Arabi Uniti sono almeno 19 le leggi che trattano o contengono temi relativi alla protezione dei dati personali; la costituzione del Paese, il codice penale, il *Cyber Crime Law* e normative di settore che hanno ripercussioni sul sistema sanitario, sull'*e-commerce* ed in altre industrie nazionali prevedono disposizioni in materia di *privacy*, nonché pene per la violazione delle relative normative. All'inizio del 2021, l'*Abu Dhabi Global Market* (ADGM)[2] ha sostituito il ADGM *Data Protection Regulation* del 2015 con una serie di leggi che concentrano maggiormente la loro attenzione sul tema della responsabilità del trattamento dei dati, con requisiti simili a quelli previsti dal GDPR.

1 Bahrain, Kuwait, Oman, Qatar, Arabia Saudita, Emirati Arabi Uniti

2 Centro finanziario internazionale e zona franca situata sull'isola di Al Maryah nella capitale degli Emirati Arabi Uniti

L'area del *Dubai International Finance Center* (DIFC) ha previsto, inoltre, l'applicazione dal 1 luglio 2020 della legge n.5/2020 per la salvaguardia dei dati individuali processati dalle entità che agiscono nell'area DIFC. Tra i requisiti principali richiesti dalla normativa ritroviamo l'obbligatorietà di trasparenza nei confronti dei titolari dei dati acquisiti, l'applicazione di strutture adeguate per la condivisione di informazioni con le autorità governative, nonché l'introduzione di un *framework* che permetterà la cooperazione ed il trasferimento di dati tra il DIFC, l'Unione Europea ed il Regno Unito.
Nel novembre 2021 il governo dell'emirato ha approvato la legge federale n.45/2021 "*UAE Personal Data Protection Law*" (PDPL), entrata in vigore il 2 gennaio 2022, che ha stabilito criteri restrittivi per la *data protection* e la *privacy;* tali previsioni vengono applicate, ai sensi dell'art. 2, ad ogni soggetto con attività economica nel Paese che processi dati personali di individui residenti all'interno o all'esterno dei confini nazionali, nonché ad ogni *data processor* o *data controller* con attività al di fuori degli Emirati ma che utilizzi dati di soggetti all'interno dello Stato. Il PDPL, perciò, contiene caratteri di extraterritorialità simili a quelli previsti del GDPR. Un'eccezione è prevista al comma 2 dello stesso articolo, dove si esclude l'applicazione dei suddetti termini per gli enti pubblici quando gestiscono dati personali, sanitari o bancari disciplinati dalle rispettive legislazioni, nonché alle organizzazioni all'interno delle zone franche.

Al fine delle attività di raccolta dei dati è necessario l'espresso consenso del soggetto titolare che, come previsto dall'articolo 6 del PDPL, deve rispettare alcune condizioni necessarie:
1. Il titolare del trattamento dei dati deve dimostrare il consenso dell'interessato se il consenso è invocato come base legale per il trattamento dei suoi dati personali;
2. Il consenso può essere ottenuto elettronicamente o per iscritto, ma deve essere chiaro, semplice, inequivocabile ed accessibile;
3. Il metodo per ottenere il consenso dovrebbe includere informazioni su come l'interessato può ritirare il proprio consenso e tale procedura deve essere di facile realizzazione.
È da notare che, similmente a ciò che è accaduto in Qatar, è prevista l'emissione di *Executive Regulations* che regoleranno dettagliatamente le previsioni legislative; la necessità di tale previsione, infatti, sorge in vari casi disciplinati dalla normativa, primo fra tutti i tempi di notifica in caso di violazione, che come regolato dal PDPL dovrà avvenire immediatamente dopo la scoperta del *data breach*, lasciando, però, una carenza normativa sulle tempistiche esatte.
Il Regno dell'Arabia Saudita ha approvato con *Royal Decree* n.98/1443 del 16 settembre 2021 la legge sulla protezione dei dati personali, che trova la sua applicazione nei riguardi dei dati personali all'interno del Paese ed al trattamento delle informazioni al di fuori dei confini nazionali di soggetti residenti nel Regno. I diritti concessi agli interessati ai sensi del *Royal Decree* sono in linea con quelli concessi agli interessati ai sensi del GDPR, come il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, informazione, portabilità dei dati e opposizione. La legge ha individuato, per i primi due anni, il *Saudi Data & Artificial Intelligence Authority* (SDAIA) come l'autorità responsabile per l'implementazione delle previsioni normative, contemplando la possibilità, a seguito di sviluppi giurisprudenziali e legali, di passare le funzioni di supervisione al *National Data Management Authority* (NDMO). È interessante notare che la legge proibisce esplicitamentre la raccolta dei dati personali senza il consenso del soggetto titolare, ma prevede dei casi in cui tale obbligo può venir meno:
1. Quando le attività di raccolta sono effettuate nell'interesse del soggetto stesso ed è difficile od impossibile entrare in contatto con lo stesso;
2. Quando le attività di raccolta sono effettuate ai sensi di ulteriori previsioni normative;
3. Quando il *data controller* è un'entità pubblica e l'attività di raccolta è effettuata per motivi di sicurezza nazionale o di giustizia.

Infine, i *data controllers* saranno tenuti a conformarsi al *Royal Decree* entro un periodo di un anno dalla data della sua entrata in vigore. Per quanto riguarda le entità situate al di fuori del Regno, il loro obbligo di nominare un rappresentante nazionale e di conformarsi alla normativa sarà ritardato per un periodo massimo di cinque anni dall'entrata in vigore della norma. In questo panorama normativo si inserisce il progetto *Neom*, voluto dal governo saudita per dar vita a una grande *smart city* nel deserto, con diversi poli urbani, turistici, industriali, ricreativi e commerciali sparsi nella provincia di *Tabuk*, nel nord-ovest del Paese. Il progetto, fondato su principi di *carbon neutral* ed emissioni zero, comprende un'isola tecnologica nel Mar Rosso, *Sindalah*, una città tra le montagne, *Trojena*, un complesso urbano lungo 170 km, *The Line*, ed un polo industriale, *Oxagon*. Nell'ambizioso progetto, inoltre, è ricompreso il più grande stabilimento di produzione di

idrogeno verde, un investimento di 175 milioni di dollari in *Volocopter*, la nuova generazione di mezzi di trasporto volanti, nonché un settore di produzione cinematografica e di innovazione dei motori elettrici in collaborazione con la *McLaren*. All'interno del progetto è stato previsto anche l'implementazione di un sistema di tecnologie *blockchain*, con lo scopo di azzerare le commissioni (stimate in 25 miliardi di dollari su un totale di 650 miliardi di transazioni), per il trasferimento di denaro alle famiglie d'origine, pagate dai lavoratori migranti in tutto il mondo. Ciò che fa riflettere, però, è la decisione della Corte penale speciale dell'Arabia Saudita che ha condannato tre uomini, membri della tribù *Huawaitat,* residente da secoli nell'area dove sta sorgendo l'enorme progetto, che si sono opposti allo sgombero forzato della loro terra. Il tribunale speciale, solitamente interessato nella gestione dei casi di terrorismo, ha emesso condanne a morte nei confronti di *Shadli*, *Ibrahim* e *Ataullah al-Huwaiti*, dopo che alcuni video e foto contro il progetto erano stati pubblicati sui *social media*. Le autorità saudite hanno fatto spesso ricorso a sgomberi forzati per liberare le aree, in operazioni caratterizzate da assenza di trasparenza ed abusi, come il mancato pagamento di risarcimenti pattuiti in precedenza con la delegazione locale. Infine, l'enorme quantità di dati prodotti pone, naturalmente, interrogativi sul loro utilizzo e sulla *privacy*: come si potranno conciliare e gestire le problematiche legate alla protezione dei dati personali in un progetto dove il metaverso giocherà un ruolo chiave?

## 3. Conclusioni

Il *General Data Protection Regulation* (GDPR), regolamento cardine dell'Unione Europea in tema di *data protection* e *privacy*, rappresenta un obiettivo per i Paesi della regione del Medio Oriente e Nord Africa (MENA), per la creazione di un modello legislativo unificato per la protezione dei dati personali dei cittadini dell'area.
Le prime normative di settore dei componenti del GCC sono state influenzate dalla Direttiva CE del 1995 in tema di circolazione e trattamento dei dati personali. L'avvento e la diffusione del GDPR ha incentivato la revisione delle leggi sulla *privacy* dell'intero globo, includendo i Paesi della regione MENA. Nonostante molti governi abbiano fortemente preso in considerazione la legislazione europea in tema, le divergenze culturali, politiche e socio-economiche sono rimaste determinanti per l'approvazione delle attuali normative negli Stati mediorientali.

Un *framework* regionale armonizzato sulla protezione dei dati, però, incoraggerebbe i Paesi dell'area MENA ad incentivare un maggior accordo sul tema della *privacy* e del *data protection*, riducendo, da un lato, i vuoti legislativi di alcuni Paesi e, dall'altro, allentando le restrizioni sulla circolazione delle informazioni, conservando, però, un livello di protezione adeguato. Inoltre, l'eventuale unificazione della legislazione permetterebbe di ridurre le difficoltà negli investimenti poste dalle stringenti regole nazionali sul flusso di dati, incentivare l'integrazione e la cooperazione economica della regione, creare un ambiente più chiaro e maggiormente comprensibile nel quale possano operare le differenti organizzazioni pubbliche e private, e aiutare le entità locali nella redazioni di regolamenti che si possano integrare con maggior flessibilità e semplicità alle normative dei restanti Stati dell'area MENA.
Un primo passo verso un'armonizzazione è stato, forse, effettuato dalle Nazioni del Consiglio di Cooperazione del Golfo; nonostante i 6 Paesi abbiano sviluppato distinte normative, è possibile individuare *standards* operativi e procedimentali comuni per l'intero Consiglio:
1. Assicurare che nessun dato personale sia conservato e trattato al di fuori delle attività per le quali il dato stesso sia stato raccolto;
2. Formazione e aggiornamento continuo nell'uso dei dati ed in materia di *cybersecurity* per i dipendenti;
3. Consapevolezza dell'entità delle coperture assicurative e continua valutazione dei rischi cibernetici;
4. Costruzione di misure contingenti e di risposta in caso di incidente informatico, prevedendo l'istituzione di un *Computer Security Incident Response Team* (CSIRT).

Per la realizzazione di tale obiettivo, però, è necessario tenere in considerazione le innumerevoli difficoltà presenti soprattutto in termini di fattibilità e coordinamento tra le differenti leggi in tema di *data privacy*, nonché dovute all'assenza di tali normative in alcuni Paesi della regione; sarà fondamentale, inoltre, analizzare i costi di implementazione, le tempistiche di negoziazione e la disponibilità di requisiti tecnici e professionali per gestire ed applicare i processi in maniera univoca. Un *framework* regionale richiederà l'applicazione di principi di interoperabilità per permettere alle autorità governative e agli *stakeholders* delle organizzazioni private di condividere conoscenze, prospettive, *best practices* per armonizzare le regolamentazioni nazionali in tema di protezione dei dati individuali. ©