*Raccomandazione dell'OCSE sulla Digital Security*

"*È impossibile poter eliminare totalmente il rischio digitale, ma questa sfida può e deve essere governata in modo efficace*". Queste le parole del Garante della Privacy, nel comunicato stampa che ha seguito la pubblicazione della Raccomandazione Ocse su "Digital Security Risk Management for Economic and Social Prosperity" dello scorso 17 Settembre 2015.

**Il Garante ha accolto con dovuto interesse il documento dell'Organizzazione che prescrive l'adozione di otto step fondamentali agli stakeholders coinvolti dalla tematica della sicurezza digitale**. Considerazione questa non di poco conto se consideriamo che – parafrasando l'intervento dell'autorità italiana – il ricorso agli strumenti tecnologici innovativi, per esemplificare IoT, sanità elettronica, cloud computing, può comportare il rischio di esporre le informazioni di milioni di cittadini ad attacchi informatici, perdite o distruzioni con gravi conseguenze anche finanziarie, sulla competitività e sulla fiducia tra clienti, dipendenti, azionisti.


L'intervento dell'Organizzazione deputata a favorire la cooperazione e lo sviluppo economico ha individuato alcuni principi generali che dovranno aiutare le imprese e le istituzioni coinvolte ad implementare un modello di sicurezza digitale in grado di tutelare *in primis* i diritti degli interessati, ma anche gli interessi economici rilevanti. Lo sviluppo del mercato digitale rappresenta una parte fondamentale ed essenziale nel funzionamento delle economie globali e del progresso sociale, in grado di generare nuove opportunità di fare impresa.

Se il progresso tecnologico risulta un aspetto fondamentale per le economie mondiali, altrettanto sembra esserlo – secondo la Raccomandazione - la creazione e l'implementazione di perimetri di sicurezza delle informazioni coinvolte.

Il monito della Raccomandazione non lascia dubbi all'interpretazione e rappresenta un evidente invito nei confronti dei Governi e delle istituzioni coinvolte a farsi responsabili nella gestione del rischio in materia di sicurezza digitale, tematica questa da introdurre nella pianificazione generale.

E le istituzioni coinvolte sono molteplici: governi, organizzazioni pubbliche e private, ma anche i singoli soggetti allo stesso modo interessati da una gestione consapevole del rischio connesso al progresso tecnologico ed alla conseguente tematica della sicurezza digitale.

I principi individuati dall'Organizzazione spaziano dalla consapevolezza degli stakeholders circa le ripercussioni che i rischi informatici hanno sugli aspetti economici e sociali delle imprese. Rischi che possono essere abbattuti mediante alcuni fattori chiave: capacità, responsabilità, innovazione, prontezza e continuità delle soluzioni adottate. Il senso è quello di ridurre gli incidenti legati alla sicurezza digitale e contemporaneamente favorire il progresso economico e sociale delle attività. Tali

principi dovranno essere applicati secondo un modello di cooperazione multilivello da svilupparsi verso l'alto mediante il coinvolgimento non solo delle pubbliche istituzioni, ma anche dei singoli privati e verso l'esterno non potendo prescindere da un approccio di tipo internazionale.

Gli strumenti idonei a ridurre i rischi connessi alla sicurezza digitale sono ravvisabili nell'implementazione delle misure di sicurezza siano queste fisiche o logiche. In tale ottica, l'Ocse raccomanda l'adozione di strategie nazionali volte a creare le condizioni favorevoli per gli stakeholders, nonché nuovi standard di sicurezza da adottare a tutela delle informazioni gestite nell'attività professionale ed economica svolta.


In ragione di quanto sopra esposto, è evidente come le "regole della privacy" contribuiscano a creare un sistema più sicuro o quantomeno riducano drasticamente i rischi legati alla perdita di informazioni, aumentando sensibilmente il livello di sicurezza digitale delle medesime.

Lo scopo primario della disciplina europea (Dir. CE/95/46) e di quella nazionale (D. lgs. 196/2003) è quello di tutelare il dato personale e garantire l'esercizio dei diritti dell'interessato cui il dato personale afferisce.
Altrettanto vero è che le fonti appena citate rappresentino anche forme di tutela del know-how aziendale: tutelare la sicurezza delle informazioni necessarie al business equivale a tutelare il business stesso.

Tra gli strumenti che possono essere utilizzati per mettere in sicurezza le informazioni e ridurre i rischi derivanti da una perdita di dati vi sono le misure minime di sicurezza di cui all'Allegato B, Disciplinare Tecnico, del D. lgs. 196/2003.
Lo scopo primario di tali misure è analogo alla ratio sottesa alla Raccomandazione sulla Digital Security ovvero evitare o quantomeno ridurre al minimo il rischio derivanti dalla distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o trattamento non consentito in base alle finalità perseguite.

Tra le misure minime è opportuno menzionare:

- la predisposizione delle nomine ad incaricato del trattamento che devono essere rivolte ai soggetti che materialmente intervengono nel trattamento delle informazioni;
- la predisposizione di adeguate regole relative alla gestione delle credenziali di autenticazione ai sistemi informativi nonché di disabilitazione delle medesime qualora il soggetto assegnatario non si trovi più ad utilizzarle;
- sistemi di autorizzazione diversificati;
- la protezione degli strumenti informatici mediante aggiornamento continuo di antivirus e firewall a ciò appositamente dedicati;
- la mappatura degli amministratori di sistema interni ed esterni;
- certificazioni di conformità dei prodotti utilizzati.

Da non sottovalutare è l'adozione di regolamenti informatici aziendali che vadano a disciplinare le regole di utilizzo della strumentazione elettronica concessa in uso ai lavoratori (personal computer, posta elettronica, telefoni aziendali, rete internet) in modo da ridurre o evitare sensibili perdite di informazioni trattate ovvero conosciute mediante l'ausilio degli strumenti elettronici.

Infine, la possibilità di nominare i soggetti esterni che intervengono nella filiera del trattamento quali responsabili esterni del trattamento ai sensi dell'articolo 29 del D. Lgs. 196/2003. Tale nomina diventa uno strumento di tutela delle informazioni nel senso di strumento efficace con il quale impartire analitiche istruzioni ai soggetti che effettuano – esemplificando - attività di assistenza tecnica sui sistemi informativi aziendali.

**Ebbene, in tale ottica pare assolutamente condivisibile il contenuto della Raccomandazione Ocse sulla Digital Security**. In attesa degli interventi legislativi richiesti dalla Organizzazione, il consiglio da dare ai diversi stakeholders è quello di partire con il rispetto degli accorgimenti previsti e a tutela dei dati personali e della sicurezza digitale delle informazioni.

**Valentina Frediani**