LO SCENARIO

La sicurezza ai tempi del mobile business

Sempre più spesso al lavoro fuori ufficio, sempre più impegnati con dispositivi digitali. La crescita dei mobile workers porta con sé non solo nuove opportunità per le aziende, ma anche nuove minacce per chi non adotta misure adeguate di protezione. Mentre la normativa comunitaria sulla privacy è entrata in una nuova era, che impone un radicale ripensamento delle strategie aziendali sull'It.

Sempre più smart workers

L'architettura dei nuovi uffici dice molto dell'evoluzione in atto nel mercato del lavoro. Molte aziende che negli ultimi tempi hanno ripensato gli spazi di lavoro si sono orientate verso soluzioni che prevedono l'addio alla postazione fissa: chi arriva, si posiziona nel primo spazio libero. E numerose realtà prevedono un numero di postazioni inferiore a quello dei propri dipendenti, nella consapevolezza che quotidianamente molti di loro sono fuori ufficio.
Secondo uno studio, i lavoratori italiani dotati di device mobili per l'attività lavorativa si sono attestati a quota 11 milioni nel 2016, con una tendenza a crescere, tanto che già nel 2020 si toccherà quota 13 milioni. Su tutti gli home-based worker (professionisti in genere a partita Iva), ma sono sempre più numerosi anche gli addetti aziendali che lavorano almeno tre giorni al mese da casa a seguito di iniziative smart working più strutturate avviate dalle aziende di riferimento. In Europa, entro il 2021, si stima che i lavoratori agili saranno ben 120 milioni.

Il nuovo "ambiente" di lavoro

Questa evoluzione porta con sé un crescente scambio di informazioni su strumenti informatici, in tempo reale, abilitando nuove opportunità di business. Allo stesso tempo, però, obbliga imprese e lavoratori a gestire strumenti e procedure complesse e con un numero di variabili notevole.
Uno scenario che spiega la crescente attenzione delle aziende verso l'ambito della cybersecurity. Secondo il Norton Cyber Security Insights Report, sono oltre 16 milioni gli italiani che lo scorso anno sono caduti in trappole informatiche, un dato che costituisce oltre un terzo della popolazione adulta (37%). Le perdite nella Penisola hanno totalizzato quasi 3,5 miliardi di euro, e ogni vittima ha perso in media più di due giorni lavorativi per occuparsi delle conseguenze del crimine informatico subìto.

Il dato personale secondo le regole europee

Il tema della cybersecurity si intreccia a più riprese con le tematiche riguardanti la difesa dei dati e della privacy. Il 25 maggio è entrato in vigore il nuovo regolamento europeo in materia, noto con l'acronimo Gdpr (General Data Protection Regulation), attraverso il quale il legislatore ha introdotto regole più nette in merito all'informativa e al consenso, stabilendo precisi limiti al trattamento automatizzato dei dati, alla relativa violazione e all'interscambio degli stessi al di fuori della Comunità europea. Trattandosi di un regolamento, è divenuto immediatamente operativo, senza necessità di normativa nazionale

L'importanza della rendicontazione

Daniele Terranova, socio fondatore di Observere (società che assiste le aziende simulando i controlli operati dalla Guardia di Finanza in tema di fiscalità, privacy, antiriciclaggio e 231), sottolinea l'importanza della rendicontazione. «Le aziende dovranno essere sempre capaci di dimostrare al Garante perché, quali e come sono stati raccolti i dati personali, come sono stati protetti durante il trattamento, perché sono stati/saranno conservati un certo tempo, perché è stato giudicato lecito il trattamento, come ne è stata predisposta la trasportabilità e la cancellazione, la procedura di *data breach*, come è stata (se lo è stata) effettuata la valutazione dell'impatto privacy; come è stato (se lo è stato) elaborato, controllato e sviluppato il registro dei trattamenti; quali clausole sono state inserite nei contratti, per esempio, quelli con i responsabili come gli amministratori di sistema e altro ancora».
In sostanza, saranno il titolare e/o il responsabile del trattamento a decidere l'organizzazione da porre a protezione dei dati personali. Saranno chiamati a tracciare formalmente quanto adottato (e fatto) e pure quanto non fatto per mezzo di specifica documentazione contenente le rispettive motivazioni.
Terranova vede grandi cambiamenti anche nei rapporti tra le aziende. «Queste infatti non sono monadi a se stanti, ma comunicano costantemente con altri partner, con clienti, con istituti di credito e con molti altri soggetti commerciali e non. Nel farlo utilizzano infrastrutture dedicate o semplicemente le più comuni caselle di posta elettronica. L'essere conformi alle regole del Gdpr equivale a un cenno di assicurazione verso i terzi di una corretta gestione delle informazioni e dei dati»

di recepimento. Così in tutta l'Ue da qualche settimana esiste una comune concezione del dato personale, definita come "Qualsiasi informazione riguardante una persona fisica identificata o identificabile". Il testo precisa che "Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

La svolta del "privacy by design"

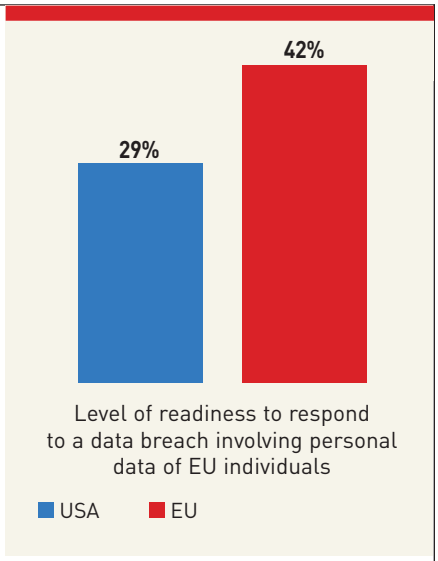
Viene inoltre definita la procedura di trattamento (del dato personale) come "Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".
Il concetto che maggiormente coinvolge la cybersecurity all'interno del Gdpr è quello della "privacy by design", che impone che il vincolo di assicurare una adeguata protezione ai dati raccolti e trattati sia affrontato sin dal momento in cui il trattamento dei dati viene progettato e definito. Le aziende devono perciò adottare misure tecniche e organizzative adeguate, operando sulla base di una corretta valutazione dei rischi. Anche se poi ciascuna realtà ha un margine di libertà per quanto riguarda la scelta delle misure da adottare per ridurre il più possibile i rischi. La cifratura figura tra le opzioni principali.

Sistema di gestione del rischio

Per Corrado Zana, responsabile cyber risk di Willis Towers Watson, è fuor di dubbio che il nuovo regolamento sia «Più severo e attento alla tutela dei dati personali del sistema legislativo che lo precede», dato ad esempio che introduce sanzioni amministrative che hanno un impatto importante in caso di inosservanza. Tuttavia, l'aspetto più innovativo per l'esperto risiede nel vincolo di mantenere nel tempo un sistema adeguato di protezione della privacy. «Non è quindi sufficiente l'implementazione *una tantum* di un elenco corposo di controlli, ma è necessario predisporre e documentare l'esistenza di un sistema di gestione del rischio privacy, in grado di intervenire dinamicamente al variare delle condizioni di rischio, per definire e mettere in campo le contromisure di volta in volta più adeguate».

Nuovi strumenti e nuove figure

Un passaggio essenziale della nuova normativa comunitaria riguarda il data privacy impact assessment, strumento essenziale per dare corso al nuovo approccio alla protezione dei dati personali basato sul principio di responsabilizzazione. «Consiste in un processo mirato a valutare l'impatto sulla privacy delle varie categorie di informazioni di cui si dispone e l'efficacia dei sistemi di trattamento e controllo atti a proteggerle», sottolinea Zana.
Che non trascura anche il cambio di rotta imposto dalla previsione di nominare un data protection officer, figura specialistica dotata di competenze sia in ambito normativo, sia in materia di protezione dati. Questa figura diventa obbligatoria per le autorità e gli organismi pubblici, quando i trattamenti richiedono il monitoraggio sistematico su larga scala e quando il trattamento riguarda su larga scala i dati sensibili.



Banche e Tlc avvantaggiate

Secondo un recente studio condotto da Ponemon Institute (v. grafico a fianco), intervistando un migliaio di aziende europee e americane, appare che solo il 30% ritiene di essere conforme a tale requisito già alla data del 25 maggio, riscontrando appunto come molto complessa la costruzione di una capacità di notifica dell'evento alle autorità ed eventualmente ai diretti interessati.
Sempre nello stesso studio è riportato che la quota di aziende europee e statunitensi che si considerano conformi alla data fatidica del 25 maggio varia dal 40 al 60%, con istituzioni finanziarie e aziende tecnologiche in lizza per la prima posizione.
«Non stupisce che le banche e gli operatori Tlc siano stati i più reattivi – sottolinea il responsabile cyber risk di Willis Towers Watson –. La conformità al Gdpr richiede la messa a punto di un sistema specifico di risk management dedicato alla privacy, sistema del tutto analogo a quelli già presenti appunto con maggiore frequenza in ambito finanziario e tecnologico».