Dato il progressivo aumento dei soggetti interessati alla protezione dei propri dati personali, le imprese stanno curando in via sempre maggiore le informazioni che raccolgono investendo soprattutto in misure di sicurezza efficienti atte a proteggere i dati trattati attraverso l'utilizzo di strumenti aziendali. Tuttavia **molto spesso si tralascia un aspetto fondamentale per garantire il corretto utilizzo dei dati personali: la formazione dei dipendenti**. Mentre il focus principale delle aziende è nei confronti dei soggetti terzi rispetto all'impresa, infatti, poca attenzione viene riservata agli *insider* (M. Stonebraker, "State of the Art of Big Data Technology, Big Data Privacy Workshop, 2014).

Le minacce che possono derivare dall'attività dei lavoratori sono due: la diffusione, volontaria o meno, delle informazioni e l'utilizzo erroneo delle stesse.

Un corretto utilizzo dei mezzi a propria disposizione da parte dei dipendenti è essenziale al fine di evitare *data breach*. È infatti possibile che i lavoratori utilizzino strumenti personali per svolgere alcune attività lavorative, dall'accesso a servizi di *cloud storage* all'invio di una mail con l'account aziendale, anche solo per ragioni di efficienza. Questa pratica, che prende il nome di *Bring Your Own Device* (BYOD) può essere regolata con apposite policy al fine di gestire gli accessi ai servizi aziendali attraverso l'installazione di software di *Mobile Device Management* (MDM) (D. A. Flores, et al. "Bring your own disclosure: analysing BYOD threats to corporate information", 2016 IEEE Trustcom/BigDataSE/ISPA)**.**

Anche a seguito di ciò, tuttavia, è opportuno assicurarsi che il lavoratore utilizzi il *device* in modo corretto impostando una *password* a protezione dello strumento in caso di furto dello stesso ed evitando, ad esempio, di connettersi a reti pubbliche.

Dal punto di vista giuridico il legislatore cerca di risolvere il problema della possibilità di un erroneo utilizzo dei sistemi informatici agendo su diversi fronti.

In prima battuta **per gli incaricati**, ovvero "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile" (art. 4, lett. h, cod. privacy) **devono essere previsti**

dei limiti relativi al tipo e alla quantità di dati a cui hanno accesso in base ai loro compiti all'interno della struttura aziendale. Questa norma prevede, quindi, un obbligo per le imprese di permettere l'accesso ai dati solo a soggetti che, per via delle loro mansioni, abbiano competenze specifiche che garantiscano la tutela della privacy degli interessati.

Tale volontà del legislatore è confermata dall'art. 39, comma 1, lett. a, Regolamento UE 2016/679 (di qui in poi GDPR) laddove viene assegnato al DPO il compito di formare e sensibilizzare il personale che partecipa ai trattamenti e alle connesse attività di controllo (G. Machì, "La figura del Data Privacy Officer in azienda", Bollettino Adapt 16 gennaio 2017, n. 2).

Tuttavia, sebbene sia necessario che ogni lavoratore sappia, ad esempio, quali siano i rischi di utilizzare strumenti diversi rispetto a quelli previsti dalle policy, **talvolta una formazione eccessiva può essere controproducente**. Un certo livello di inconsapevolezza rispetto alle modalità di funzionamento è, anzi, richiesto per evitare che il processo utilizzato possa essere volontariamente guidato verso un determinato risultato.

Data la veloce evoluzione scientifica in questa campo è impossibile prevedere un'attività formativa una tantum: essa deve necessariamente ricomprendere degli aggiornamenti periodici.

La formazione permette ai lavoratori di essere coscienti degli oneri connessi all'attività di trattamento dei dati, tuttavia, all'atto pratico, permane il rischio che essi non seguano le direttive poiché le attività che devono essere svolte sono ritenute poco efficienti. Anche su questo versante il GDPR offre degli spunti.

L'art. 25, reg. 679/2016 rubricato "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita", prevede che al fine del soddisfacimento dei requisiti del regolamento e della tutela dei diritti degli interessati debbano essere messe in atto "misure tecniche ed organizzative adeguate". Alla luce di questa norma **è quindi possibile estendere il concetto di privacy by design oltre la mera previsione di strumenti tecnici** che, ad esempio, permettono

attraverso un input di disconnettere il device, **ed includervi anche l'organizzazione dei processi aziendali** affinché i lavoratori si comportino in modo tale da diminuire i rischi derivanti dal trattamento.

A tale scopo **sarebbe opportuno cercare di integrare in modo efficace le attività svolte per tutelare la privacy con il resto delle mansioni eseguite dai singoli lavoratori**. Oltre all'utilizzo di policy e sanzioni disciplinari potrebbe venire in aiuto la stessa *big data analytics* e, più in particolare, la *User Behaviour Analytics* (UBA) (B. Dickson, "How data science fights modern insider threats", techcrunch, 2016) vale a dire lo studio del comportamento degli utenti nell'utilizzo di *software* o *hardware*. Analizzando il comportamento dei lavoratori durante l'utilizzo degli strumenti di lavoro sarebbe possibile creare dei nudge (K. Yeung, "'Hypernudge': Big Data as a Mode of Regulation by Design", Information, Communication & Society, 2016) ovvero delle particolari scelte organizzative che permettono di indirizzare il comportamento dei lavoratori stessi senza imporre loro degli obblighi. Ovviamente una attività di analytics di questo tipo dovrebbe essere posta in essere nel rispetto non solo della disciplina privacy, ma anche di quella relativa ai controlli sui lavoratori (E. Dagnino, "People Analytics: lavoro e tutele al tempo del management tramite big data", LLI vol. 3, n. 1, 2017).

Un cambiamento di questo genere è sicuramente oneroso per le imprese, tuttavia, il mercato dei dati personali è particolarmente influenzato dalla fiducia dell'utenza che è più propensa a dare il consenso al trattamento dei propri dati personali ad imprese considerate affidabili. **Un investimento sulla formazione dei lavoratori che svolgono attività di trattamento di dati personali, quindi, oltre che garantire l'adempimento al nuovo regolamento 679/2016 potrebbe produrre, nel lungo periodo, vantaggi sul versante economico.**

Gaetano Machì

ADAPT Junior Fellow

@gae95

Scarica il **PDF**