Privacy e lavoro agile, limiti e regole per il trattamento dei dati



*La rubrica "**Digital & Law**" è curata da **D&L Net** e offre una lettura delle materie dell'innovazione digitale da una prospettiva che sia in grado di offrire piena padronanza degli strumenti e dei diritti digitali, anche ai non addetti ai lavori. Per consultare tutti gli articoli clicca qui.*

*Articolo a cura della dott.ssa **Flavia Piscitelli**, giurista e componente del D&LNET*

L'uso scorretto degli strumenti di lavoro porta a delle conseguenze negative. Prendiamo come riferimento un recente caso con protagonista un impiegato della **Banca Comercială Română** (BCR) che per agevolare i clienti nella gestione delle pratiche usava il proprio cellulare per farsi inviare tramite WhatsApp le copie di documenti e carte d'identità, violando non solo le policy interne della banca, ma anche diverse disposizioni del **GDPR**.

Con la progressiva affermazione della modalità di lavoro

“smart” anche nel nostro Paese, caratterizzata dall’utilizzo, sempre più frequente, di strumenti elettronici e da un aumento esponenziale della circolazione di dati e informazioni, è necessario promuovere non solo la conoscenza degli strumenti, ma soprattutto garantire la sicurezza dei trattamenti di dati effettuati per il tramite di piattaforma web, social network e strumenti di messaggistica.

Ma quali sono i limiti e le regole da tenere in considerazione?

Il cattivo uso degli strumenti di lavoro: il caso dell’impiegato della BCR

Nel caso del dipendente della BCR, la decisione di adottare WhatsApp per comunicare con la clientela risulterebbe del tutto autonoma e arbitraria. In effetti, l’impiego dei canali social e/o di strumenti di messaggistica per la comunicazione con l’esterno compete in ogni caso al Datore di lavoro/Titolare del trattamento. Da quest’ultimo dipende anche la valutazione dei rischi per le libertà e i diritti delle persone fisiche in relazione ai trattamenti di dati personali dei clienti (interessati al trattamento) effettuati tramite tali strumenti, nonché le misure organizzative e tecniche da adottare.

È importante quindi disciplinare l’utilizzo degli strumenti attraverso policy interne e indicando le specifiche misure di sicurezza organizzative e procedure a cui si devono poi attenere i dipendenti autorizzati al trattamento dei dati dei clienti.

Nel caso specifico, e a seguito dell’istruttoria portata avanti dal Garante privacy rumeno, l’Autorità ha riscontrato la violazione delle disposizioni in materia di sicurezza del

trattamento (art. 32 del GPPR) irrogando alla Banca una sanzione amministrativa di 24.163,50 lei (5000 euro).

L’uso degli strumenti elettronici e il ruolo del datore di lavoro

In tema di utilizzo di strumenti elettronici nel contesto lavorativo è utile considerare quanto indicato dell’Autorità Garante per la protezione dei dati personali nelle Linee guida per posta elettronica e internet, che dettano regole precise per il datore, da adottare per garantire il corretto uso degli strumenti elettronici e il corretto trattamento dei dati nel contesto lavorativo.

Stando a quanto prescritto dal Garante, il datore di lavoro può certamente adottare misure opportune per evitare usi impropri della navigazione in internet, quali ad esempio la configurazione di sistemi o l’utilizzo di filtri che prevengano determinate **operazioni reputate incompatibili con l´attività lavorativa** (quali l´upload e/o il download di file o software aventi particolari caratteristiche o anche l´accesso a determinati siti da inserire in una sorta di black list).

Il controllo degli strumenti aziendali rientra infatti tra le facoltà del datore di lavoro che, per motivi di sicurezza, può monitorare l’uso dei computer e dei devices aziendali in dotazione dei dipendenti.

È pur vero che il personale deve essere sempre preventivamente informato del possibile controllo, delle modalità e dalle ragioni che lo giustificano. La cattiva gestione degli strumenti da parte di un dipendente potrebbe infatti ledere il rapporto di fiducia con l’azienda e dunque comportare una giusta causa di licenziamento.

BYOD: l’utilizzo degli strumenti personali nel contesto lavorativo

Un fattore da non trascurare è l’intensificarsi dell’utilizzo di dispositivi mobili personali (pc, tablet, smartphone, ecc.) per lo svolgimento dell’attività lavorativa (cd. BYOD, acronimo di “Bring Your Own Device”). Sebbene l’utilizzo di queste soluzioni sia indubbiamente conveniente, questo potrebbe comportare inevitabilmente rischi per la protezione dei dati personali.

Sul tema è intervenuto il Garante Europeo per la Protezione dei dati (**GEPD**) che attraverso l’emanazione delle Linee Guida sull’utilizzo dei dispositivi mobili, fornisce un’analisi dei rischi generici legati al trattamento dei dati personali su dispositivi mobili, nonché raccomandazioni e migliori pratiche che dovrebbero aiutare le istituzioni dell’UE (ma anche le organizzazioni private, aziende e altri enti pubblici) a raggiungere un livello di protezione dei dati conforme al regolamento (CE) n. 45/2001[1], poi sostituito dal Regolamento (UE) 2018/1725[2].

Le Linee guida contengono alcune raccomandazioni che aiutano l’organizzazione/azienda a dimostrare la correttezza del trattamento dei dati personali sui dispositivi mobili.

Ad esempio:

1) **Coinvolgere il DPO in merito a tutti gli aspetti relativi all’introduzione e dell’uso dei dispositivi mobili** personali nell’azienda/organizzazione;

2) **Valutare caso per caso i benefici derivanti dall’uso di dispositivi mobili personali**, tenendo conto dei rischi e l’invasività che tale uso può implicare;

3)Valutare **l’adozione da parte del datore di lavoro di una policy aziendale interna che regoli i limiti e le modalità di**

utilizzo dei dispositivi mobili personali nel contesto lavorativo;

4)**Eseguire una valutazione d'impatto (DPIA**) sugli strumenti di controllo utilizzati e adottare le misure tecniche ed organizzative necessarie per garantire la sicurezza dei dispositivi mobili personali;

5)Adottare **procedure interne per la gestione delle violazioni dei dati;**

6) Impostare i dispositivi in modo tale da evitare che la raccolta e l'elaborazione di dati personali risulti "in eccesso", **nel rispetto del principio di minimizzazione dei dati;**

7) **Rispettare i principi di privacy by design previsti dal GDPR** nella definizione delle misure di sicurezza da applicare ai singoli dispositivi.

Anche nel Manuale RPD troviamo riferimenti al BYOD, dove si afferma che il DPO nello svolgimento delle proprie attività, con l'aiuto del personale informatico e della sicurezza, deve acquisire familiarità con i sistemi ICT, l'architettura e le politiche della propria organizzazione. In particolare deve valutare se tra i dispositivi utilizzati, oltre ai computer, vengano inclusi dispositivi portatili e/o mobili (e/o "dispositivi propri" del personale – **per i quali deve essere predisposta una policy "Bring Your Own Device [BYOD**]");

L'adozione di una policy interna per regolare l'utilizzo degli strumenti

La soluzione migliore sarebbe quella di prevedere un regolamento aziendale interno: uno strumento necessario atto a regolare la condotta dei lavoratori sul luogo di lavoro

e le modalità di utilizzo degli strumenti di comunicazione.

Grava quindi sul datore la responsabilità di indicare in modo chiaro e dettagliato, quali siano gli strumenti, le modalità di impiego e come vengano effettuati i controlli, in un'apposita policy interna.

Conclusioni

Elemento fondamentale per garantire il corretto uso degli strumenti di lavoro è **la formazione dei dipendenti, da parte del datore**, per quanto concerne la gestione dei dispositivi aziendali, con particolare riguardo per la protezione dei dati, evitando di adottare soluzioni "smart" che però non tengano in debito conto la protezione dei dati dei soggetti interessati dal trattamento.

---

[1] Regolamento (CE) n. 45/2001, del 18 dicembre 2000, del Parlamento Europeo e del Consiglio, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

[2] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

*Articolo a cura della dott.ssa **Flavia Piscitelli**, giurista e componente del D&LNET*

> *Privacy e lavoro agile, limiti e regole per il trattamento dei dati*