SMART WORKING E PROTEZIONE DEI DATI PERSONALI

Indicazioni operative per un corretto trattamento di dati personali nel contesto dello "smart working"

Con riferimento alla Circolare n. 1/2020 del 04/03/2020 ("Misure incentivanti per il ricorso a modalità flessibili di svolgimento della prestazione lavorativa") emanata dal Ministro per la Pubblica Amministrazione, nella quale si dispone il ricorso in via prioritaria alle modalità di "lavoro agile" o "smart working" nel contesto delle misure di contenimento dell'emergenza epidemiologica da Covid-19, si fornisce una serie di **indicazioni operative per il trattamento di dati personali** effettuato con queste modalità di svolgimento della prestazione lavorativa.
Innanzitutto, i dipendenti devono svolgere i trattamenti previsti dalle rispettive mansioni **nel rispetto delle prescrizioni e indicazioni operative contenute negli atti di individuazione quali persone autorizzate al trattamento**, ai sensi dell'art. 29 del RGPD ("Regolamento Generale sulla Protezione dei Dati"). Tali prescrizioni, aventi carattere "generico" anche allo scopo di adattarsi a situazioni emergenziali come quella in cui ci troviamo, sono perfettamente valide anche in un contesto di "smart working". Nel rispetto della sopracitata circolare ministeriale e la conseguente esigenza di regolamentare modalità lavorative che, di fatto, costituiscono una novità per la pubblica amministrazione, comprese le istituzioni scolastiche, ribadiamo in questa sede alcuni concetti fondamentali e necessari al fine di effettuare un trattamento di dati personali conforme alla vigente normativa in un contsto di "smart working".
Indipendentemente dalle diverse concrete vie di implementazione dello "smart working", avendo necessariamente a che fare con dispositivi informatici, è necessario che il lavoratore **garantisca un adeguato livello di protezione di tali dispositivi**, attenzionando in particolare il rispetto dei principi di integrità, riservatezza e disponibilità dei dati e delle informazioni ivi contenute, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi. A tale scopo occorre:

1. proteggere l'accesso ai dispositivi informatici (computer, tablet, smartphone) e delle connessioni (cablate o Wi-Fi) attraverso l'**uso di password sufficientemente robuste e sicure**: a tal proposito si consiglia di utilizzare password lunghe in quanto più difficili da scoprire e prive di riferimenti ai dati anagrafici propri e dei familiari; ciò vale tanto per l'accesso ai propri dispositivi quanto per l'accesso a Internet, in quanto la diffusa prassi di non cambiare la password di default per l'accesso alla rete Wi-Fi è una delle

principali cause di accessi non autorizzati alla rete locale e, di conseguenza, a dati e informazioni potenzialmente sensibili;

2. prediligere, ove possibile, l'**utilizzo di sistemi di autenticazione a due fattori**: Google permette di utilizzare l'autenticazione a due fattori per tutti i propri account, i quali sono la chiave di accesso, oltre agli account Android, anche agli strumenti di G Suite;
3. **mantenere aggiornati sistemi operativi e software**, sia desktop che mobile, utilizzati per svolgere la prestazione lavorativa: gli aggiornamenti sono importanti in quanto spesso risolvono falle di sicurezza sfruttabili per accedere ai dispositivi e ai dati in essi contenuti;
4. **utilizzare e mantenere aggiornati specifici software antivirus e firewall**, che offrono una tutela nei confronti dei rischi normalmente connessi alla navigazione in rete: i sistemi operativi Windows hanno integrati sia un sofware antivirus (Defender) sia un firewall;
5. **implementare sistemi di backup** per assicurare la disponibilità di dati e informazioni in ogni momento, sia tramite sistemi cloud che tramite dispositivi di archiviazione di massa come hard disk portatili e chiavette USB: in entrambi i casi l'accesso ai dati va protetto adeguatamente, magari servendosi di soluzioni crittografiche;
6. nel lavorare da casa è altresì importante **attuare una serie di misure organizzative** per svolgere le proprie mansioni in un ambiente lavorativo idoneo, come avere cura nell'impostare la propria postazione di lavoro, non lasciare incustoditi i dispositivi e non condividere informazioni riservate con i propri familiari.

Le indicazioni sopra esposte valgono per qualsiasi tipo di concreta applicazione dello "smart working". Nel caso in cui tale modalità di svolgimento della prestazione lavorativa è messa in atto tramite l'**utilizzo dei propri dispositivi personali**, così come riconosciuto nella circolare ministeriale alla quale facciamo riferimento vista la cronica non sufficiente disponibilità di risorse e strumenti informatici, tali indicazioni devono essere **seguite con particolare rigore**. Vanno altresì seguite nel caso in cui l'istituzione scolastica sia in grado di fornire ai propri dipendenti dei dispositivi scolastici opportunamente configurati secondo le misure minime di sicurezza ICT per la PA.

Passando a modalità di "smart working" più avanzate, si rammenta che nel caso in cui sia possibile per i lavoratori effettuare l'accesso alla rete interna della scuola dall'esterno, ciò va fatto necessariamente tramite una **VPN**, vale a dire un collegamento privato crittografato e, quindi, sicuro. Vanno evitate modalità che garantiscono standard di sicurezza molto inferiori

come l'apertura di porte. Il vantaggio di accedere alla rete interna dell'Istituto è facilmente comprensibile, ma deve essere fatto in assoluta sicurezza.

Una soluzione che unisce le potenzialità di condivisione di dati e informazioni in tempo reale (così come avviene in un sistema server-client come quelli che caratterizzano le reti interne degli Istituti) e le possibilità di coordinamento, gestione e rendicontazione del lavoro svolto da remoto è quella di servirsi di **servizi cloud**, così come suggerito nella stessa circolare del Ministero. Servizi cloud come quelli messi a disposizione a titolo gratuito per le istituzioni scolastiche da Google e Microsoft – ma anche la suite Argo Software e le varie piattaforme di e-learning accessibili via web sono servizi cloud – sono potenti strumenti che permettono la gestione digitale dell'attività amministrativa e didattica delle istituzioni scolastiche. Anche in questo caso valgono le indicazioni di cui sopra, specialmente quelle riguardanti la **robustezza delle credenziali** per accedere a tali servizi. Inoltre, quando ci si rivolge a servizi esterni, bisogna sempre ricordare che questi agiscono quali responsabili esterni del trattamento, ai sensi dell'art. 28 del RGPD: è ormai prassi consolidata che siano direttamente le grandi aziende a formalizzare questo tipo di rapporto nei contratti di servizio che si sottoscrivono alla registrazione, ma è sempre meglio andare a verificare leggendo attentamente la documentazione fornita.

Infine, si segnala che il Garante per la protezione dei dati personali ha raccomandato ai titolari del trattamento, quali le istituzioni scolastiche, di astenersi dall'effettuare **iniziative autonome di raccolta sistematica e generalizzata di dati riguardanti lo stato di salute dei lavoratori** che non siano normativamente previste o disposte dagli organi competenti. Operazioni di questo tipo devono essere svolte da soggetti che istituzionalmente esercitano queste funzioni in maniera qualificata, come gli operatori sanitari e il sistema attivato dalla protezione civile. **Resta comunque fermo l'obbligo del lavoratore di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sul luogo di lavoro**. A riguardo, il Ministro per la Pubblica Amministrazione ha fornito indicazioni operative sull'obbligo per il dipendente pubblico di segnalare all'amministrazione la provenienza da un'area a rischio.