Smart working e tecnologia informatica nella Pubblica Amministrazione

di Luigi Buonomo [*]

"Non possiamo affrontare il futuro con una Pubblica Amministrazione del passato" è una citazione dell'ex presidente degli Stati Uniti, Barack Obama, che invitava a riflettere su quanto fosse necessario che la Pubblica Amministrazione si attrezzasse per affrontare sfide sempre più complesse avviando un importante processo di innovazione culturale, istituzionale e organizzativo.

La lentezza con la quale questo processo di innovazione stava e sta tuttora procedendo in Italia, ha mostrato i suoi effetti in relazione allo smart working, diventato modalità ordinaria di svolgimento della prestazione lavorativa nelle Pubbliche Amministrazioni (art. 84 DL n. 18/2020) a seguito dell'emergenza epidemiologica da SARS-CoV-2. Questa circostanza ha impresso una sostanziale accelerazione tanto all'attivazione di questa modalità lavorativa, estesa al pubblico impiego con la Legge n. 124/2015 e declinata in dettaglio con la Direttiva n. 3 del 2017 del Presidente del Consiglio dei ministri, quanto, più in generale, al percorso di trasformazione digitale, anch'esso invero già previsto dal legislatore a partire dal 2005 con l'emanazione del D.Lgs. n. 82/2005.

Il tutto, però, è avvenuto in assenza della adeguata progettazione, sperimentazione, comunicazione, sensibilizzazione, formazione e monitoraggio che questo modello organizzativo richiede. Infatti, occorre subito chiarire che fare smart working è cosa diversa dall'inviare una e-mail ovvero dall'accendere una webcam per fare una video conferenza. Fare smart working vuol dire predisporre una infrastruttura hardware e software compatibile con il lavoro fuori sede, investire sulla crescita delle competenze digitali del dipendente, organizzare il lavoro in modo nuovo ridefinendo i processi di misurazione e valutazione della performance.

Le componenti infrastrutturali

Per quanto attiene alle componenti infrastrutturali, bisogna distinguere tra quelle hardware e software: tra le prime rientrano tipicamente i Personal Computer ovvero i dispositivi ad essi assimilabili e la connettività di rete; tra le seconde le applicazioni di collaborazione, di elaborazione di dati e quelle gestionali tipiche di ciascuna Amministrazione.

In primo luogo, il lavoro agile presuppone che il dipendente disponga di una **adeguata connettività di rete**. Se infatti il Personal Computer (ovvero altri dispositivi analoghi) può essere anche fornito dall'Amministrazione di appartenenza, la connettività è tipicamente onere dello smart worker e, da un punto di vista tecnologico, è ciò che lo distingue dal telelavorista di cui alla Legge n. 191/98 (c.d. Bassanini-ter).

L'adeguatezza della connettività, benché sia una variabile essenziale, esula spesso dall'ambito di discrezionalità sia del dipendente che dell'Amministrazione. Per la maggior parte degli applicativi gestionali che scambiano dati sulla rete è sufficiente una connessione c.d. a banda larga, ma, per utiliz-

zare strumenti di virtual collaboration, appare necessario avere una connessione a velocità superiore. Da questo punto di vista, le statistiche più recenti indicano che in Italia la c.d. banda ultralarga raggiunge solo il 24% della popolazione contro la media UE del 60%; per gli altri smart worker bisogna sperare che il proprio luogo di lavoro domestico sia raggiunto da un ponte radio 4G e affidarsi alla connessione radiomobile. Inoltre, in molti casi, la disponibilità di una connessione alla rete internet sconta, oltre che carenze infrastrutturali, la necessità di gestire la **concorrenza di esigenze divergenti** in ambito domestico: la stessa connessione infatti deve essere utilizzata da tutti i membri della famiglia e, a seconda delle applicazioni utilizzate, il "consumo" di banda da parte di una di queste può impedire quasi completamente il funzionamento delle altre concorrenti.

Riguardo ai device utilizzati per lo smart working è necessario approfondire gli impatti che gli stessi hanno nell'ambito della sicurezza informatica e della salute del lavoratore.

Per quanto concerne l'ambito della **sicurezza informatica**, occorre distinguere se il dispositivo utilizzato è personale o fornito dall'Amministrazione. In questo secondo caso molte misure di sicurezza, normalmente adottate a livello centralizzato come firewall, aggiornamenti di sicurezza e di firme antivirus, permangono anche nell'utilizzo fuori ufficio. Nel caso in cui, invece, lo smart worker utilizzi dispositivi personali come previsto anche dalla direttiva 1/2020 emanata dal Dipartimento della Funzione Pubblica -pratica conosciuta come Bring Your Own Device (BYOD), si pone il problema di garantire livelli di sicurezza e protezione adeguati alle esigenze e alle modalità di fruizione del parco applicativo dell'Amministrazione.

In quest'ottica, il Cert-PA, organismo dipendente da AgID e quindi dalla presidenza del Consiglio dei ministri, ha pubblicato un vademecum per aiutare i dipendenti pubblici a utilizzare in maniera sicura pc, tablet e smartphone personali quando lavorano da casa. Si tratta di **undici semplici raccomandazioni** rivolte alle persone che hanno adottato la modalità di lavoro agile elaborate sulla base delle misure minime di sicurezza informatica per le Pubbliche Amministrazioni fissate dalla circolare 1/2017 del 17 marzo 2017.

Le raccomandazioni sono le seguenti:

- "Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione.
- Utilizza i sistemi operativi per i quali attualmente è garantito il supporto.
- Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo.
- Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati.
- Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione.
- Non installare software proveniente da fonti/repository non ufficiali.
- Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro.
- Non cliccare su link o allegati contenuti in e-mail sospette.
- Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette.
- Collegati a dispositivi mobili (Pen-Drive, HHD-esterno, etc.) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione).
- Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa."

Tra le raccomandazioni elencate appaiono maggiormente significative quelle di cui ai punti 2,3 e 6. Se infatti le altre richiamano norma-

li comportamenti che siamo abituati a tenere, l'utilizzo di dispositivi di proprietà è strettamente connesso con la possibilità di installare software non istituzionali e sconta la possibilità che tali strumenti non siano recenti ed utilizzino pertanto sistemi operativi obsoleti. È stato verificato che sono soprattutto i software provenienti da fonti/repository non ufficiali –e principalmente i giochi- a contenere malware in grado di raccogliere dati in modo invisibile al proprietario stesso. Il possesso di computer domestici ormai obsoleti ma sufficienti per l'uso domestico che ne fa un utente naturalmente non digitale, porta con sé l'impiego di sistemi operativi -come ad esempio Windows 7 e XP- per i quali non sono più previsti aggiornamenti di sicurezza.

In ogni caso, non bisogna dimenticare che, al di là delle problematiche informatiche, al dipendente in smart working sono richiesti gli usuali comportamenti finalizzati a ridurre i rischi connessi alla diffusione di dati riservati già adottati anche in ufficio.

Infine, si evidenzia che, esiste una specie di **trade-off tra sicurezza informatica e salute del lavoratore**, in riferimento alla postazione di lavoro, questo in quanto i dispositivi assegnati dall'Amministrazione sono tipicamente dei laptop e come tali comportano maggiori difficoltà nel rispettare le prescrizioni previste dal D.Lgs. n. 81/2008 in materia di videoterminali (l'INAIL ha espressamente indicato che "le attività connesse all'uso del computer portatile rientrano in quelle tutelate dal titolo VII relativo ai videoterminali").

A tale proposito, si ricorda che, quando si prevede di dover effettuare un lavoro prolungato con un PC portatile, è bene munirsi e fare uso di una tastiera esterna, di una base -in modo da sollevare lo schermo- e di un mouse. L'adozione di un mouse al posto del touchpad e di una tastiera ergonomica favoriscono, infatti, l'appoggio di entrambi gli avambracci attenuando il sovraccarico degli arti superiori, riducendo l'angolazione dei polsi e conseguentemente l'affaticamento dei tendini della mano. Inoltre, è bene usare uno schermo esterno se i caratteri sullo schermo del computer portatile sono troppo piccoli.

Accanto alla dotazione hardware, perché lo smart working sia efficace, è essenziale la disponibilità di una efficiente **infrastruttura applicativa**.

Se le operazioni tipicamente svolte in smart working si limitano alla predisposizione in autonomia di atti, piuttosto che a rispondere a richieste di chiarimento da parte dell'utenza, gli

strumenti di ***office automation*** (Office 365, Apache OpenOffice, etc) insieme ad un client di posta elettronica appaiono più che sufficienti. In questo caso anche la connettività di rete non è un elemento critico.

Se la predisposizione degli atti avviene in forma collaborativa ovvero se allo smart worker è richiesto di partecipare a riunioni e gruppi di lavoro, allora è necessaria l'introduzione degli strumenti sopra richiamati di ***virtual collaboration*** (Teams, Slack, WebEx, etc.), dove una adeguata connettività di rete è necessaria al loro pieno utilizzo. Queste applicazioni permettono di organizzare delle riunioni video con condivisione dei documenti e possibilità di lavorare contemporaneamente su uno stesso file ovvero di archiviarlo in cartelle condivise, nonché di gestire agende di lavoro. Si evidenzia come questa modalità di interazione sia diventata obbligatoria per le udienze sia civili che penali durante il periodo di emergenza da COVID-19 a seguito dell'approvazione, da parte di CSM e CNF, di due protocolli che declinano le modalità di attuazione delle norme contenute nel D.L. n. 18/2020 in materia di udienze civili tramite collegamento da remoto, udienze civili tramite trattazione scritta e video conferenza nel sistema penale.

Un livello superiore di efficienza dell'infrastruttura applicativa è rappresentato dall'**informatizzazione dei processi operativi**, rispetto alla quale la digitalizzazione dei provvedimenti amministrativi rappresenta la parte preponderante della Pubblica Amministrazione. Tra gli esempi più noti di questo fenomeno si ricorda il "protocollo informatico", di cui al DPR 445/2000 e la digitalizzazione delle procedure giudiziarie, meglio nota come "Processo Civile Telematico", ma più in generale si fa riferimento a tutti quegli applicativi gestionali che supportano le Amministrazioni nella produzione dei loro output tipici. Oltre ai generici vantaggi legati alla digitalizzazione degli atti, qui assunti come dogma per necessità di sintesi, in

relazione allo smart working occorre evidenziare che l'informatizzazione permette di effettuare controlli sui processi più efficaci in relazione alla misurazione della performance individuale -e conseguentemente organizzativa- sganciando definitivamente così la valorizzazione delle capacità e delle competenze dei dipendenti dalla loro presenza sul luogo di lavoro.

Dal un punto di vista tecnico, però, perché ciò sia possibile, occorre verificare che gli applicativi gestionali in parola siano stati progettati per essere resi disponibili anche fuori dall'ufficio. Similarmente, i portali intranet dovrebbero essere trasformati in aree riservate all'interno dei siti internet, in modo che tutte le funzioni e le informazioni veicolate per il loro tramite possano essere fruite anche senza connessione alla rete LAN.

Anche in questo caso, il problema si pone soprattutto in ottica di sicurezza informatica e la scelta di quale soluzione adottare per rendere tali applicativi disponibili da remoto dipende anche dal tipo di tecnologia sottostante gli stessi. L'accesso da remoto ad applicativi dedicati, siano essi in versione correnti che legacy[1], può essere garantita dall'implementazione di adeguati sistemi di **sicurezza perimetrale** ovvero dall'utilizzo di connessioni virtuali, note come VPN[2], o ancora tramite l'evoluzione di queste ultime rappresentata dalle così dette **"scrivanie virtuali"** (VDI)[3]. In alcuni casi, per processi standardizzati, quali a titolo di esempio quelli di gestione del personale e quelli del ciclo di acquisto, potrà essere valutata anche l'adozione del modello **SAAS** (Software As A Service)[4].

Ognuna delle soluzioni sopra elencate presenta un trade-off tra sicurezza informatica e costo di implementazione, costo da considerare sia in termini economici che di tempo necessario per l'implementazione stessa. Tutte queste soluzioni necessitano di una pianificazione e solo in rarissimi casi sono realizzabili in breve tempo; in altre parole, bisogna iniziare a pensare ai sistemi informatici perché possano sempre essere nativamente fruiti all'esterno dell'organizzazione.

Se per i processi interamente interni all'Amministrazione le soluzioni infrastrutturali sopra indicate garantiscono la possibilità di lavorare da remoto, differente è la questione quando l'atto si forma secondo un iter che coinvolge soggetti esterni e in particolare quando a questi viene chiesta l'apposizione di una sottoscrizione autografa per rendere l'atto prodotto giuridicamente valido (si pensi tanto ai procedimenti amministrativi ad istanza di parte quanto, ad esempio, a quelli conciliativi) In questo caso la telematizzazione del processo e la possibilità che lo stesso sia realizzato internamente da remoto, appare molto più complessa. La soluzione è rappresentata dalla possibilità di firmare elettronicamente gli atti.

Il Regolamento UE 910/2014 (Regolamento eIDAS), all'art.3, paragrafo 1, n. 10 fornisce la definizione di firma elettronica: "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare." Oltre alle firme elettroniche cd. "semplici", la normativa disciplina ulteriori tipologie di firme che assicurano in modo crescente la certezza del soggetto firmatario, nonché la sicurezza di un determinato documento elettronico. Si possono così incontrare: la firma elettronica avanzata (FEA) e quella qualificata (FEQ).

Il problema è che più aumenta la sicurezza fornita dalla firma digitale, più aumenta la complessità di gestione di tali firme e più diminuisce la probabilità che il comune cittadino o il piccolo imprenditore (con accezione atecnica) che intende accedere ai servizi della Pubblica Amministrazione da remoto ne rimanga escluso.

A favorire la diffusione della firma digitale degli atti, è intervenuta AgID con la recente determinazione n. 157/2020 del 23 Marzo 2020 recante le "Linee Guida per la sottoscrizione elettronica di documenti ai sensi dell'art. 20

del CAD" con la quale, all'esito del percorso di consultazione pubblica che si è svolto dal 21 novembre al 28 dicembre 2019, è stato formalmente riconosciuto allo SPID anche il valore giuridico di sottoscrizione autografa, in conformità all'articolo 20 del Codice dell'Amministrazione Digitale per la firma di atti e contratti[5].

L'introduzione di questa nuova modalità di firma, così come l'utilizzo della Firma Elettronica Avanzata -altra modalità più facilmente utilizzabile dal comune cittadino- comportano però per la Pubblica Amministrazione la necessità di reingegnerizzare i propri sistemi al fine di permettere agli stessi di integrare questi sistemi di firma e telematizzare effettivamente i procedimenti coinvolti.

Le competenze digitali

26 anni fa nasceva un tormentone pubblicitario passato alla storia e adottato nel linguaggio comune: "La potenza è nulla senza controllo". Oggi, volendo parafrasare il messaggio potremmo dire "l'infrastruttura è nulla senza le competenze per usarla" e tale frase appare tanto banale quanto attuale in riferimento allo smart working imposto a seguito del lockdown. Molte Amministrazioni si sono trovate ad implementare software collaborative senza la possibilità di organizzare corsi di formazione sugli stessi con l'effetto di avere la tecnologia a disposizione ma di non sapere come farla usare ai propri dipendenti: lo smart worker che non sa usare un tale prodotto ovviamente non può fruire di corsi di formazione sullo stesso, tramite il medesimo strumento.

Al di là del momento contingente, un'adeguata **formazione sulle competenze digitali** appare imprescindibile se si ammette che le tecnologie digitali sono condizione necessaria per permettere alle persone di svolgere il proprio lavoro da remoto; ma quale tipo di formazione e quale tipo di competenze sono richieste? Per attivare correttamente lo smart working non viene certamente chiesto al dipendente pubblico di possedere competenze sull'area SMAC (Social, Mobile, Analytics, Cloud), o quelle su Intelligenza Artificiale, Robotica, IoT o la Cybersecurity. Sono, invece, necessarie quelle individuate come Digital Soft Skills e definite dal Parlamento Europeo nel 2006 (Raccomandazione del Parlamento Europeo e del Consiglio del dicembre) come "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa

è supportata da abilità di base nelle TIC (Tecnologie dell'Informazione e della Comunicazione): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".

Oggi, considerato il quasi decennale blocco del turnover e un approccio sostanzialmente giuridico-amministrativista del "recruiting" nella PA, fattori che hanno portato ad avere, in media, un personale scarsamente "digitalizzato", appare necessario investire nella formazione di competenze digitali come sopra declinate. A tale proposito, l'Ufficio per l'innovazione e la digitalizzazione del Dipartimento della funzione pubblica, ha curato la realizzazione di un documento che descrive l'insieme minimo delle conoscenze e abilità che ogni dipendente pubblico, non specialista IT, dovrebbe possedere per partecipare attivamente alla trasformazione digitale della Pubblica Amministrazione, il **Syllabus**. Organizzato in cinque aree tematiche e tre livelli di padronanza, questo documento dovrebbe rappresentare lo strumento di riferimento sia per l'attività di autoverifica delle competenze digitali che per la definizione di corsi volti a indirizzare i fabbisogni formativi rilevati.

Quale futuro per lo smart working post COVID-19 e il ruolo dell'ICT

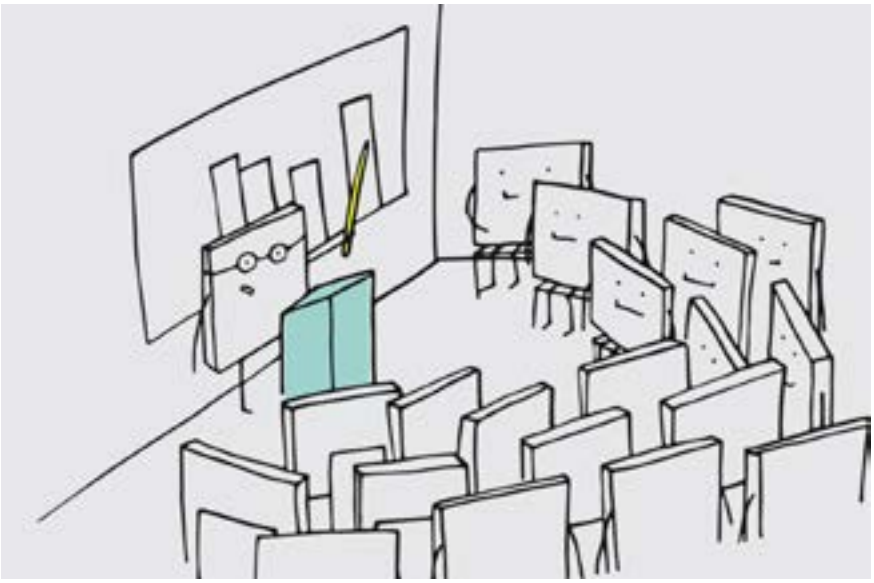
Quella che stiamo vivendo è una sperimentazione su larga scala di una specie particolare di smart working, in realtà coincidente con l'home working, nato all'insegna dell'urgenza e dal "fai da te". Con lo smart working non dovrebbe essere semplicemente cambiato l'indirizzo in cui viene effettuata la prestazione lavorativa, ma dovrebbe cambiare la modalità di effettuazione della prestazione stessa, che deve passare dalla semplice presenza sul luogo di lavoro all'orientamento per obiettivi. Pensare che l'informatica debba supportare lo smart working sempli-

cemente fornendo strumenti di collaborazione a distanza, ad esempio per fare una video-riunione virtuale o per condividere documenti su uno spazio cloud, vuol dire perdere una grande opportunità. L'ICT, attraverso la telematizzazione dei servizi erogati all'utenza e la digitalizzazione delle procedure interne può, da un lato, produrre un servizio migliore al cittadino e dall'altro fornire gli strumenti affinché la prestazione del dipendente pubblico possa essere sganciata dalla semplice presenza in ufficio e misurata e valutata secondo reali parametri di efficacia ed efficienza.

Perché ciò avvenga è necessario però:

- progettare correttamente le infrastrutture hardware e software affinché queste siano effettivamente disponibili anche fuori dall'ufficio;
- investire sulle competenze digitali di base, sia in termini di formazione del personale già presente nell'amministrazione, che introducendo tra i parametri di selezione del personale entrante il possesso delle Digital Soft Skills come sopra definite;
- misurare e valutare la performance -sia individuale che organizzativa- in ragione dell'efficienza nella produzione degli output e dell'efficacia degli outcome rispetto agli stakeholder esterni.

Ma quest'ultimo punto, e più in generale la progettazione sia informatica che organizzativa dello smart working, presuppone un ripensamento delle modalità con cui i dirigenti pubblici devono esercitare il proprio ruolo, un ripensamento che metta al centro la produzione di valore, la profonda conoscenza dei processi operativi della propria Amministrazione, la capacità di valutare la misurazione informatizzata di output e outcome. ■



Note

[1] Nella prassi informatica, si definisce legacy un'applicazione obsoleta ma che continua ad essere utilizzata in quanto non sostituibile nel breve tempo ovvero per la quale è iniziato un processo di reingegnerizzazione ancora da completarsi.

[2] Una VPN (Virtuale Private Network) simula, tramite applicativi software di criptaggio dei dati, la connessione tra computer remoti come fossero collegati da reti fisiche dedicate (LAN). Tramite la VPN il dipendente in smart working può raggiungere gli applicativi normalmente visibili solo tramite rete Intranet anche per mezzo di una normale connessione internet. Le VPN presentano, però, elevati livelli di rischio per la sicurezza in ragione della possibilità di violare l'intera rete dell'Amministrazione attraverso la semplice compromissione di un singolo dispositivo utilizzato dai dipendenti.

[3] Rispetto alla classica VPN, le "scrivanie virtuali" (VDI) utilizzano fattori di autenticazione a più livelli che impediscono l'intercettazione delle credenziali di accesso al sistema quando il dipendente si connette da remoto, rendendo la connessione stessa più sicura.

[4] Con il modello SAAS un provider di servizi fornisce le applicazioni direttamente tramite Internet, le Amministrazioni si abbonano al software e accedono a esso tramite il web o servizi di integrazione applicativa del fornitore stesso.

[5] Si evidenzia che, come precisato dal Consiglio di Stato – le Linee Guida adottate dall'Agenzia per l'Italia Digitale, ai sensi dell'articolo 71 del CAD, hanno carattere vincolante e assumono valenza erga omnes. Nella gerarchia delle fonti, le Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute.

[*] Dirigente dell'Ispettorato Nazionale del Lavoro. Le considerazioni contenute nel presente articolo sono frutto esclusivo del pensiero dell'autore e non hanno carattere in alcun modo impegnativo per l'Amministrazione cui appartiene