Unicredit: Byod, ci risiamo

Sul portale aziendale nei giorni scorsi è stata pubblicata la news in cui si propone, alle lavoratrici/lavoratori, l'utilizzo del proprio dispositivo personale, che sia cellulare/tablet, per lavorare, che l'azienda definisce come *"fidato"*, al posto degli ingombranti dispositivi forniti dall'azienda (cit. da portale) ….

Sul tema queste Organizzazioni Sindacali erano intervenute, quando l'iniziativa era stata adottata per l'area Digital, ponendo una serie di rilievi che riproponiamo:

- **Gli strumenti di lavoro devono essere forniti dal datore di lavoro**, le norme della legge 81 del 22/5/2017 e dell'art 39 del CCNL anche questa volta non vengono menzionate, L'unico obiettivo è il risparmio dei costi da parte aziendale per la fornitura degli "ingombranti dispositivi"
- **Non è vero che si puo` lavorare da qualsiasi luogo**, l'Art. 39 del CCNL e precise regole aziendali sul lavoro agile vietano i luoghi pubblici come luogo di lavoro.

La presentazione sul portale aziendale del BYOD, fa apparire questa modalita`di utilizzo dei dispositivi digitali come un grande vantaggio per le/i lavoratrici/tori: mentre il vantaggio è aziendale dal punto di vista del risparmio sui costi di acquisto dei dispositivi, per il collega il risparmio è nello spazio nello zaino….

Inoltre, non si chiarisce minimamente come vengono trattati i dati personali in relazione alla privacy. Dal nostro punto di

vista, l’introduzione del BYOD si raffigura come un nuovo trattamento e questo non puo` prescindere da un suo esame approfondito in relazione al rischio privacy sottostante.

Nelle istruzioni viene poi detto che non sara` possibile richiedere il porting del proprio numero privato sulla SIM aziendale.

Non si chiarisce cosa succede in caso di perdita del proprio dispositivo personale – se non che non si possa utilizzare un dispositivo ad uso temporaneo o richiedere quello aziendale – e, in merito ai rischi correlati, si rimanda alla policy aziendale.

Inoltre, nulla si dice sul diritto alla disconnessione, poiché difficilmente ci si disconnette dal proprio cellulare, né tantomeno dallo smart watch e quindi si rimane raggiungibili a qualunque ora del giorno e della notte, quando siamo in ferie o altro.

Non sono previsti rimborsi per l’utilizzo e l’usura dei dispositivi personali e/o della sim.

Durante l’emergenza pandemica si era reso indispensabile, in alcuni casi, l’utilizzo di dispositivi personali, ma ora l’emergenza è finita e deve finire anche questa modalita` di risparmiare sui costi.

In sintesi, non si puo` sollecitare lavoratrici/lavoratori ad effettuare la prestazione lavorativa senza fornire loro gli adeguati strumenti, invitandoli all’utilizzo del proprio dispositivo personale!!!

Milano, 22 giugno 2023

Le Segreterie di Coordinamento delle OO.SS. di Gruppo Unicredit
FABI – FIRST/CISL – FISAC/CGIL – UILCA – UNISIN

Gruppo Bper: attenti a ciò che andiamo a guardare

In questi giorni diverse filiali stanno ricevendo chiamate dall'Ufficio preposto ai controlli sulla Privacy nelle quali si chiede conto di interrogazioni effettuate su rapporti di clienti, **apparentemente non giustificate dall'operatività ordinaria**.

La questione è estremamente seria e non va assolutamente sottovalutata.

Le modalità di accesso ai dati personali furono disciplinate dall'accordo sottoscritto in data 29 settembre 2014 che prevede, in sostanza, che **l'accesso ai dati della clientela non possa avvenire se non per finalità strettamente connesse all'attività lavorativa**. In base all'accordo sono stati disposti controlli automatici volti all'individuazione di comportamenti anomali. In caso di anomalie viene informata la Direzione Risorse Umane di Gruppo, che provvede a contattare il dipendente al quale viene chiesto di fornire giustificazione, eventualmente assistito da un rappresentante sindacale. **In questa fase l'Azienda non può avviare provvedimenti disciplinari.**
La mancanza di adeguate giustificazioni, tuttavia, può comportare conseguenze potenzialmente non meno gravi: **l'Azienda è tenuta ad informare il titolare del rapporto** oggetto di interrogazioni anomale per comunicargli l'accesso illecito a i suoi dati, aprendo la strada a possibili segnalazioni al Garante per la Privacy dalle quali possono derivare pesanti sanzioni ed anche possibili richieste di risarcimento danni.
Un'eventuale sanzione comminata dal Garante per la Privacy

legittimerebbe – a posteriori – un provvedimento disciplinare, che a quel punto potrebbe essere anche molto importante.

Le novità introdotte dall'accordo, resosi **necessario a seguito di specifica prescrizione da parte del Garante per la Privacy**, furono illustrate con **Circolare 28 del 30/9/2014**: si tratta pertanto di una norma piuttosto datata, che, ad onor del vero, fino ad oggi non aveva generato particolari problemi.

Nei mesi scorsi, tuttavia, si è verificata un'intensificazione dei controlli, preannunciata dalla notizia di gruppo ***"Accessi impropri a dati della clientela da parte dei dipendenti"***, pubblicata lo scorso 30 novembre. Da allora abbiamo notizie di numerose richieste di chiarimenti arrivate alle filiali, anche a fronte di una singola interrogazione relativa ad un conto di altra dipendenza.
Come a volte accade, le disposizioni emanate da Bper si prestano ad interpretazioni a posteriori che potrebbero penalizzare i colleghi. In particolare, la disposizione dice che *"le consultazioni di dati e stampe relative a posizioni di clienti devono sempre ed esclusivamente essere svolte **in relazione alla cliente assegnata**".*
Cosa s'intende per clientela assegnata? Solo i clienti della filiale (nonostante la circolarità prevista dalle procedure)? O i clienti appartenenti al proprio modello di servizio? O solo quelli ricompresi nel proprio **portafoglio?** *(Esempio: se il direttore chiede al cassiere di predisporgli inquiry su una posizione su cui il direttore sta istruendo pratica di affidamento, che succede?)*

E' indispensabile che Bper faccia chiarezza su questo punto.

In attesa di chiarimenti, riteniamo opportuno fornire alcuni consigli volti ad evitare le gravi conseguenze che potrebbero derivare, anche in totale buona fede, da comportamenti poco attenti.

- **Non effettuare alcun tipo di interrogazione sui rapporti**

della clientela se non giustificata da finalità operative, o riferibile a motivazioni di servizio *(come riporta la citata notizia del 30/11/22).*

- Se un cliente si reca allo sportello soltanto per **richiedere un estratto conto,** senza effettuare operazioni contabili dalle quali emergerebbe in modo indiscutibile la sua presenza in filiale, è opportuno farsi firmare **una richiesta scritta** (in modo particolare se si tratta di correntisti presso altre dipendenze o di clienti che non si recano spesso in banca) corredata da fotocopia di un documento. E' indubbiamente un aggravio dell'operatività, ma sempre nella notizia del 30/11 si fa espresso riferimento alla necessità di acquisire **richieste documentabili, preventivamente autorizzate dal cliente.**
- **Non comunicare alcuna informazione per via telefonica né tramite email**. Il divieto, già presente in diverse disposizioni aziendali, viene ribadito con forza nella Notizia di Gruppo del 21/10/2022 intitolata: **"Bsecurity: chiamate di finti agenti delle forze dell'ordine".** Ricordiamo inoltre che **è vietato effettuare disposizioni ricevute attraverso richieste telefoniche o per email, fatte salve le eccezioni previste dalla circolare n. 305 del 14/12/2015** (accettazione in via del tutto eccezionale, preventiva acquisizione lettera di manleva, invio disposizioni via PEC, richiesta conferma telefonica). Invitiamo i colleghi a leggere la circolare, insieme con la notizia di Gruppo **"Regole per un corretto utilizzo della posta elettronica aziendale"** pubblicata in data 23/12/2021.
- **Non dare inizio all'istruttoria di un finanziamento senza prima aver acquisito la firma del cliente** sul modello di richiesta. In assenza di tale sottoscrizione, qualsiasi interrogazione sulle banche dati è **illegittima** e può giustificare contestazioni da parte del cliente.

In chiusura, riteniamo opportuno ricordare che la stessa legge

sulla Privacy, che ci impone doveri ben precisi, **ci offre anche alcune tutele e diritti non meno importanti**.

L'Azienda è legittimata all'utilizzo dei nostri dati personali solo in relazione agli adempimenti connessi al rapporto di lavoro. In tutti gli altri casi, **i nostri dati sensibili non possono essere diffusi.**

A titolo di esempio, costituiscono dati sensibili il fatto di beneficiare di **permessi ai sensi della L.104**, le **patologie** da cui si è affetti, la stessa **iscrizione ad un'Organizzazione Sindacale**. L'eventuale diffusione di questi dati da parte di componenti aziendali costituirebbe una violazione della nostra privacy.
Sono dati sensibili, e in quanto tali assolutamente riservati, anche i nostri risultati individuali: **nessuna normativa ne autorizza la diffusione**. Esiste, in tal senso, un pronunciamento del Garante per la Privacy che vieta la condivisione di risultati individuali anche in presenza di consenso scritto da parte dei dipendenti, vista l'evidente difficoltà di opporre un rifiuto ad un'eventuale richiesta del genere.
Eppure, capita che vengano diffuse tra le filiali classifiche nominative con numeri o percentuali di raggiungimento degli obiettivi. **Comportamenti del genere sono vietati, e devono essere immediatamente segnalati.**
Tale divieto vale anche per citazioni pubbliche in positivo, del tipo: *"Complimenti al collega John Smith per aver piazzato 5 polizze sanitarie nel mese appena trascorso!"* Ignorare questo tipo di messaggi – comunque finalizzati ad alimentare invidie e competizioni malsane tra i colleghi – significherebbe preparare la strada a comunicazioni di ben diverso tenore.

Laddove abusi relativi alla comunicazione di risultati individuali ci siano stati comunicati, siamo spesso riusciti ad ottenere la tempestiva cessazione degli stessi. Per questo la raccomandazione che ribadiamo è sempre la stessa:

consultatevi con il vostro rappresentante Fisac ogni volta che lo riteniate opportuno.

Coordinamento Fisac/Cgil Gruppo Bper

Cassazione: legittimo il licenziamento del bancario che spia i conti dei clienti Vip

La Suprema corte, sentenza n. 34717 depositata oggi, ha respinto il ricorso di un addetto al servizio clienti allontanato per "accesso abusivo al sistema informatico"

È legittimo il **licenziamento** del 'bancario' che si metta a curiosare tra i **conti** correnti dei **Vip** in assenza di qualsivoglia autorizzazione. Lo ha stabilito la **Sezione Lavoro** della Corte di cassazione, sentenza n. 34717 depositata oggi, rigettando il ricorso un addetto al servizio clienti della filiale **Unicredit** di Foggia.

A seguito di una segnalazione da parte della Outgoing Foreign Payments Office di UBIS (società del gruppo UniCredit), la banca, avuto contezza del comportamento scorretto e dell'assenza di alcuna autorizzazione, aveva contestato al dipendente "l'**accesso abusivo** o comunque non consentito,

al **sistema informatico** della Banca per controllare decine di schede-cliente di **personaggi dello spettacolo** carpendone quindi i dati sensibili". E poi lo aveva licenziato.

Il dipendente era stato poi reintegrato dal **Tribunale di Foggia** ma la **Corte di appello di Bari**, rovesciando il verdetto, aveva confermato il licenziamento, condannandolo anche alla restituzione delle eventuali somme percepite a titolo indennitario. Proposto ricorso in Cassazione, aveva sostenuto, tra l'altro, che siccome la banca non aveva in alcun modo protetto i dati contenuti nella "scheda cliente", egli aveva ritenuto di "non violare i dati sensibili altrui".

Per la Suprema corte però il motivo non convince: "Il potere di disporre di strumenti informatici volti al compimento delle operazioni finanziarie presso un istituto bancario – si legge nella sentenza – **non è di certo sinonimo di accesso indiscriminato** a banche dati. Né si può ritenere, nel caso di specie, che sussista un **onere di impedire l'accesso** a tali dati da parte della banca, che, stante il **rapporto fiduciario** tra datore e prestatore di lavoro, conceda l'utilizzo di tali strumenti informatici ai propri dipendenti affinché operino in maniera lecita durante la prestazione lavorativa".

Bocciata dunque definitivamente la tesi del ricorrente che, scrive la Corte, "ancora una volta, tenta di invocare una sorta di esimente per elidere l'illiceità del suo comportamento, **imputando paradossalmente alla banca** la mancata predisposizione di adeguate protezioni dei dati dei clienti".

Fonte: ntpulsdiritto.ilsole24ore.com

Banca Fucino: uso dispositivi personali e tutela dati sensibili dei lavoratori

Banca del Fucino S.p.A.

Spett.le Banca del Fucino S.p.A.

C.A. del Presidente

Dott. Mauro Masi

C.A. del Vice-Presidente

Dott. Francesco Maiolini

C.A. del Vice Direttore Vicario

Dott. Andrea Colafranceschi

C.A. del Responsabile Risorse Umane

Dott.ssa Roberta Pennacchietti

e p.c.

a tutte le Lavoratrici e a tutti i Lavoratori

della Banca del Fucino

Roma, 24 giugno 2020

OGGETTO: DISPOSITIVI PERSONALI E DATI SENSIBILI DEI LAVORATORI

Egregi Signori,

facciamo seguito alle ns. del 27/02 (Uso di dispositivi personali e richiesta dati sensibili) e del 5/03 (Censimento operazioni CQS e dati sensibili), per tornare sugli argomenti in essi trattati.

Ci sono infatti giunte segnalazioni dai Lavoratori che anche nel corso relativo ai prodotti di “Oltre assicurazioni”, nonché sul portale “Over” di collocamento degli stessi, si fa richiesta di **dati sensibili dei Dipendenti e del loro numero di cellulare.**

Ribadiamo che la richiesta di dati sensibili può essere giustificata solo da precise norme di legge e non da eventuali raccolte di dati per scopi commerciali o di altro tipo.
Inoltre **il numero di cellulare è personale e non può essere imposto ai Lavoratori di fornirlo per motivi lavorativi, né, tantomeno, possono essere messi a loro carico i costi di conversazione e/o di utilizzo dei dati di navigazione internet per esigenze lavorative**. Per queste due ultime occorrenze devono essere forniti dispositivi aziendali provvisti di scheda telefonica e traffico dati. Tali dispositivi, per quanto sia superfluo rammentarlo, dovranno essere **attivati esclusivamente durante l’orario lavorativo** e, in nessun caso, essere utilizzati come strumento di reperibilità oltre l’orario suddetto.

In attesa di Vs. riscontro scritto porgiamo distinti saluti.

C.A.C. Fisac Cgil – R.S.A. UILca
Banca del Fucino S.p.A.

ALLEGATI:

- Lettera su utilizzo dispositivi
- Censimento operatori CQS

Poste Italiane, così il Governo Monti ha venduto i dati degli studenti

La carta IoStudio Postepay, che dovrebbe avere funzione primaria di carta dello studente, è una prepagata che viene rilasciata senza alcuna informativa sui costi (che pure ci sono) e con un esplicito invito agli studenti ad attivarla, caricarla e iniziare a utilizzarla negli esercizi convenzionati, negli store online e anche a contribuire attivamente a estendere la rete degli esercenti.

Gli **studenti** e i loro **dati**? Sono stati venduti dal **Ministero dell'Istruzione** a **Poste Italiane**.

E non si tratta di un modo di dire: dal 2014 tutti i ragazzi e le ragazze che frequentano il primo anno delle scuole superiori ricevono in automatico la cosiddetta **Carta dello Studente**, denominata **IoStudio Postepay** con funzionalità incorporata di **carta prepagata** utilizzabile anche sul **circuito Visa**. La carta, che viene emessa dal gruppo Poste Italiane, viene consegnata in automatico agli studenti dalle **segreterie scolastiche** senza una lettera di accompagnamento ai genitori e senza spiegazione alcuna: l'unica cosa – molto evidente – è che si tratta di uno strumento di pagamento. La sua funzionalità di Carta dello Studente, ossia di carta di riconoscimento da utilizzare per usufruire di **gratuità o sconti** per l'ingresso ai musei e alle iniziative culturali è – per usare un eufemismo – messa in secondo piano.

Come si è arrivati a tutto questo?
Bisogna tornare al 2013 e al **governo Monti**: fu l'allora ministro dell'Istruzione, **Francesco Profumo**, a decidere di vendere i dati degli studenti a un operatore finanziario in cambio dell'emissione delle carte e di una **quota delle**

commissioni da versare a un apposito **fondo "per l'accesso al diritto allo studio**". In questo modo il Ministero risparmia i soldi per la stampa dei tesserini che attestano la qualifica di studente in Italia e all'estero e incamera anche qualche "spicciolo".

L'operatore finanziario in questione – Poste Italiane che si è aggiudicata la "**gara di sponsorizzazione gratuita**" indetta dal Miur (ministero dell'Istruzione, dell'Università e della Ricerca) nel 2013 – guadagna un **parco di alcune centinaia di migliaia di potenziali nuovi clienti** ogni anno. Ma un'operazione che a prima vista potrebbe parere vantaggiosa per tutti – e che viene addirittura spacciata dal ministero come *"una opportunità ulteriore a sostegno della **mobilità dello studente** ed in linea con i programmi di sensibilizzazione dei giovani cittadini e delle famiglie verso i temi dell'educazione finanziaria e dell'utilizzo responsabile e consapevole della moneta elettronica e dei sistemi digitali di pagamento"* – è in realtà solo e soltanto una **scandalosa operazione di marketing di Stato** a danno dei ragazzi e delle famiglie.
Una "pesca a strascico" che porta moltissime famiglie ad attivare anche su pressione dei figli proprio quella carta, peraltro non richiesta. Come se i comuni distribuissero ai cittadini **carte d'identità "sponsorizzate"** da questo o quell'altro istituto di credito e utilizzabili come strumento di pagamento e le Regioni facessero altrettanto con le **tessere sanitarie** (forse, dati i tempi che corrono, ci arriveremo).

Altro che educazione finanziaria e utilizzo responsabile della moneta elettronica: la carta IoStudio Postepay viene rilasciata senza alcuna **informativa sui costi** (che pure ci sono) e con un esplicito invito agli studenti ad attivarla, caricarla e iniziare a utilizzarla negli esercizi convenzionati, negli store online e anche a contribuire attivamente a estendere la **rete degli esercenti** segnalandoli all'emittente affinché possa stipulare apposite convenzioni.

Delle attività culturali e degli utilizzi a fini di istruzione della Carta dello Studente non si trova traccia nel foglio che viene rilasciato agli studenti con attaccata la loro personale IoStudio Postepay. Per contro, compare una dicitura sinistramente simile a quella del "**gioco responsabile**" che accompagna tutte le pubblicità di lotterie, gratta e vinci, scommesse e giochi d'azzardo: *"Per usare responsabilmente la tua carta IoStudio Postepay visita la sezione **IoApprendo>Educazione Finanziaria** sul Portale dello Studente*".

Come sottolinea Poste Italiane, *"Tutta l'attività di consegna e comunicazione è a cura del Ministero che è il soggetto emittente della carta e che ha predisposto il materiale di comunicazione per gli studenti e le stesse famiglie*", dunque anche i testi del foglio con cui viene consegnata la carta. Poste Italiane, poi, tiene a precisare che "*la **funzionalità di pagamento** è facoltativa e non è attiva al momento della consegna delle Carte. Per le carte emesse fino allo scorso anno la funzionalità di pagamento poteva essere attivata direttamente on line, tramite il sito dello stesso Miur.*
*A seguito del cambiamento della normativa, in particolare con l'introduzione della **IV Direttiva anti riciclaggio**, per le carte di nuova emissione sarà possibile procedere all'attivazione delle stesse solo in Ufficio Postale a seguito dell'identificazione dello studente e di un genitore, nel caso di studente minorenne*".

Dal canto suo, il Ministero dell'Istruzione ribadisce che l'attivazione della funzionalità di carta prepagata rappresenta *"esclusivamente un **servizio aggiuntivo** la cui attivazione non è obbligatoria ai fini dell'accesso alle offerte IoStudio*" e che l'emissione della carta "*è automatica ai soli fini di attestare lo status di studente e accedere a sconti e agevolazioni relativi a beni e servizi di natura culturale, a servizi per la mobilità nazionale e internazionale, ad ausili di natura tecnologica per lo studio e per l'acquisto di materiale scolastico".*

Belle parole, peccato che le cose stiano diversamente come attestano anche le parole dell'allora amministratore delegato di Poste Italiane quando il **10 aprile 2013** presentò l'iniziativa assieme al ministro Profumo: *"Con questa Carta dello Studente con la funzione della Postepay ci rivolgiamo agli studenti per consegnare loro uno* ***strumento sicuro e innovativo*** *da usare per depositare i risparmi, le borse di studio scolastiche, le paghette ricevute dai genitori"*. Significativa anche la chiosa del ministro Profumo: *"È poi di particolare significato che una parte dei proventi ricavati da Poste attraverso l'utilizzo delle funzioni di pagamento della carta contribuiranno all'istituzione del Fondo per il Diritto allo Studio, che sosterrà la realizzazione e la promozione dei progetti nazionali per l'accesso allo studio"*.

Insomma, si tratta di un vero e proprio **accordo finanziario** tra Ministero e Poste che passa sopra la testa di tutti e che elude anche la **legge sulla privacy**, dato che le famiglie non sono nemmeno chiamate a prestare il loro consenso al trattamento dei dati dei propri figli per finalità commerciali da parte del ministero (quale è a tutti gli effetti l'emissione di una carta-prodotto finanziario), in quanto – come risponde il Miur – i dati acquisiti con l'iscrizione online al sistema scolastico vengono **trasmessi in automatico** dall'Anagrafe nazionale studenti a Poste Italiane.

Fonte: www.ilfattoquotidiano.it