PRIVACY DEL LAVORATORE

Garante per la protezione
dei dati personali
Provvedimento 26 marzo 2020, n. 65

Ornella Girgenti
Avvocato giuslavorista

Uso personale di internet al lavoro, controlli datoriali solo con informativa

Il Garante per la privacy fa chiarezza sui doveri del datore in merito alle policy di utilizzo del computer aziendale per motivi aziendali. Il reclamo della lavoratrice al Garante si innesta nel giudizio di impugnazione del licenziamento per giusta causa a seguito di accesso alla cronologia internet del suo pc e seguente contestazione degli accessi a facebook e siti extra lavorativi

Il Garante Privacy, con il provvedimento del 26 marzo 2020 n. 65, interviene in materia di trattamento di dati personali effettuato attraverso l'accesso alla cronologia del pc aziendale e ad altri dati raccolti nel corso del rapporto di lavoro della reclamante. Si tratta di un argomento che trova le sue fonti di disciplina nell'ordinamento europeo e in quello nazionale e che tiene banco sempre più spesso nelle sedi giudiziarie del lavoro.

Il provvedimento del Garante

Il provvedimento in oggetto riguarda il reclamo di una lavoratrice licenziata per giusta causa a seguito di accessi a internet avvenuti durante l'orario di lavoro con utilizzo del pc in dotazione.

La reclamante ha sottoposto al giudizio del Garante plurime condotte poste in essere dalla società:

- accesso alla cronologia internet in assenza di divieto di utilizzo dei beni aziendali per fini personali;
- copia su chiavetta USB di parte dei files personali contenuti nel pc in dotazione;
- diniego di accesso alla casella di posta aziendale per estrapolare la corrispondenza personale;
- mancata consegna di tutti i documenti personali presenti negli spazi utilizzati in azienda oltre che della versione integrale dell'agenda cartacea in uso.

All'esito dell'istruttoria il Garante ha ritenuto illecita la condotta del datore di lavoro sotto tutti i profili evidenziati dalla lavoratrice e quanto ai dati estratti dal pc in dotazione (cronologia internet, files personali salvati su disco fisso, email personali) ha considerato determinante la mancata adeguata informazione circa le modalità di effettuazione dei controlli datoriali («*l'accesso al PC assegnato alla reclamante, in assenza della medesima, è avvenuto senza che all'interessata fosse stata fornita un'idonea informativa. Infatti l'informativa individuale, sottoscritta dalla reclamante … non contiene alcuna indicazione sull'uso della posta elettronica, dell'accesso ad internet e degli altri strumenti di lavoro, né sulla tipologia di controlli che il datore di lavoro si riserva di attivare*»).

Precisamente, il Garante ha ritenuto esistere la violazione dell'obbligo di fornire l'informativa all'interessato previsto dall'art. 13 Regolamento, del principio generale di correttezza dei trattamenti di cui all'art. 5, par.1, lett. a) e c), Regolamento e dei criteri di legittimazione dell'art. 6 Regolamento, oltre la violazione dell'art. 4, legge n. 300/1970 come modificato dal D.Lgs. n. 151/2015[1].

1. *In merito alle ulteriori violazioni si riportano di seguito i passaggi salienti della decisione:*

a) accertato che «la società … ha effettuato l'accesso al PC fornito in uso alla reclamante estraendo la cronologia degli accessi a Internet resa disponibile da Google Chrome. L'accesso da parte del datore di lavoro è stato consentito dalla condivisione della password di accesso tra la reclamante e il superiore», è stata riscontra la violazione dell'art. 33 d.lgs. n. 196/1993 (di seguito Codice privacy) e degli artt. 5 e 32 Regolamento UE 2016/679 (di seguito Regolamento) in quanto la condivisone della password è in contrasto con «l'obbligo di adottare misure di sicurezza volte ad assicurare "un livello minimo di protezione dei dati personali"»;

b) accertato che la società ha riscontrato solo in parte le istanze di accesso presentante dalla reclamante («accesso ai dati contenuti nel PC ad

In questa sede viene in rilievo innanzitutto l'art. 4 S.L. secondo il quale il datore di lavoro potrà utilizzare le informazioni raccolte con gli strumenti di controllo a distanza (comma 1) e con gli apparecchi di cui ha dotato i propri dipendenti (comma 2) solo per i fini connessi al rapporto di lavoro, e purché i lavoratori siano informati adeguatamente sulle modalità d'uso di tali strumenti e sui modi con cui verrà esercitato il controllo stesso.

Il controllo in questione dovrà quindi rispettare la disciplina prevista dal Regolamento (UE) 2016/679 sulla privacy (General Data Protection Regulation) e dal D.Lgs. n. 196/2003 (il Codice Privacy) così come modificato dal D.Lgs. n. 101/2018.

Ebbene, premesso che l'informativa, in quanto tale, non richiede alcuna accettazione dei lavoratori che ne sono destinatari, le questioni che si pongono, affinché l'informativa possa considerarsi adeguata, attengono al contenuto e alle modalità con le quali essa deve essere portata a conoscenza del personale dipendente.

Per quanto riguarda l'adeguatezza del suo contenuto, esso deve riguardare le modalità d'uso degli strumenti e l'effettuazione dei controlli.

È dunque onere del datore di lavoro identificare le modalità di utilizzo dello strumento che comportano l'acquisizione dei dati relativi all'attività del lavoratore.

L'informazione deve essere mirata e non generalizzata. Tale informazione dovrà riguardare gli strumenti utilizzati dal lavoratore consentendo la puntuale conoscenza dei controlli al quale quest'ultimo è assoggettato.

Informazione e controllo nella giurisprudenza della CEDU

Il provvedimento del Garante oggetto di esame si colloca nel solco tracciato dalla giurisprudenza della Corte Europea dei Diritti dell'Uomo che espressamente richiama in motivazione.

In particolare si tratta della decisione resa nella causa B rbulescu c. Romania (ricorso n. 61496/2008).

Dapprima con la sentenza del 12.1.2016 la CEDU era giunta alla conclusione che un datore di lavoro può licenziare il proprio dipendente a seguito di controlli – a distanza - effettuati sugli strumenti di comunicazione utilizzati dal lavoratore.

In particolare, l'ingegnere rumeno ricorrente era stato licenziato per inadempimento contrattuale provato dall'utilizzo per fini personali, in orario di lavoro, della chat aziendale su internet (cfr. sentenza Camera Alta: "*su richiesta del suo datore di lavoro, al fine di rispondere alle richieste dei clienti, ha creato un account di messaggistica istantanea utilizzando Yahoo Messenger … ed era l'unica persona che conosceva la password. Disponeva altresì di un altro account personale di Yahoo Messenger*"; "*il datore di lavoro ha registrato le comunicazioni di Yahoo Messenger del ricorrente in tempo reale*" e la contestazione "*consisteva di una trascrizione dei messaggi che il ricorrente aveva scambiato con il fratello e la sua fidanzata durante il periodo in cui era stato monitorato … la trascrizione comprendeva anche cinque messaggi che il ricorrente aveva scambiato con la sua fidanzata usando il suo account personale di Yahoo Messenger*") e la Corte, nel rigettare il ricorso del lavoratore, aveva stabilito che i) pur essendo violato l'art. 8 della Convenzione (diritto al rispetto della vita privata e alla riservatezza della corrispondenza[2]), esistevano policy aziendali conosciute dal dipendente e che questi aveva violato il divieto di utilizzo dei computer e delle risorse aziendali per scopi personali; ii) il controllo dei messaggio era l'unico modo per il datore di lavoro di po-

eccezione di quelli riversati in una chiavetta USB e ad alcune pagine dell'agenda utilizzata dalla reclamante rimosse prima della consegna nonché la richiesta di verificare l'esistenza di ulteriori documenti personali all'interno della stanza a suo tempo assegnata alla reclamante»), è stata riscontrata la violazione dell'art. 2 undecies D.Lgs. n. 101/2018 per non aver indicato specifiche ragioni di tutela dei diritti riferite ai dati oggetto di istanza;

c) alla dichiarazione di illiceità del trattamento dei dati personali («il trattamento dei dati personali effettuato dalla società risulta certamente illecito ai sensi degli artt. 5 e 6 del Regolamento e configura altresì una violazione dell'art. 4 legge n. 300/1970 come modificato dal D.Lgs. n. 151/2015») e in forza dei poteri correttivi attribuiti dall'art. 58, par. 2, Regolamento, sono state ingiunte alla società plurime condotte al fine di conformare al Regolamento i propri trattamenti e, «considerato che le accertate violazioni dell'art. 5 del Regolamento sono da considerarsi gravi», è stata irrogata la sanzione amministrativa pecuniaria oltre alla pubblicazione del provvedimento sul sito Internet del Garante.

2. *Gli Stati membri e l'Unione europea sono vincolati dalle disposizioni della Convenzione europea per la salvaguardia dei diritti umani e delle libertà fondamentali che trattano in particolare della riservatezza e della libertà negli articoli 8 "diritto al rispetto della vita privata e familiare" («1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza») e 10 "libertà di espressione".*

Il principio generale di segretezza della corrispondenza copre le comunicazioni sul posto di lavoro, ed in questo ambito si considerano rientranti la posta elettronica ed i files ad essa acclusi ovvero altri sistemi di messaggistica. Ancorché il datore di lavoro risulti proprietario dei dispositivi utilizzati dal dipendente ciò non esclude il loro diritto alla segretezza delle loro comunicazioni e della loro corrispondenza.

ter verificare che i propri dipendenti svolgessero correttamente le proprie mansioni, iii) il controllo datoriale sull'attività lavorativa è legittimo nella misura in cui lo stesso non risulti strettamente sproporzionato e non eccedente lo scopo della verifica dell'adempimento contrattuale.

Successivamente, la Grande Camera CEDU, con sentenza del 5.9.2017 (richiamata dal Provvedimento n. 65/2020 in commento), capovolgendo il precedente verdetto, ha sancito che il datore di lavoro che controlla le mail dei dipendenti viola il diritto alla vita privata in quanto in caso di monitoraggio deve avvisare l'interessato e comunicare in modo chiaro la natura del controllo.

In altri termini, affinché l'accesso del datore di lavoro alla mail aziendale possa ritenersi legittimo è necessario verificare anzitutto se il lavoratore risulta avvisato dall'azienda in merito alla possibilità di controllo della sua corrispondenza, alle modalità di detto controllo e alle relative motivazioni:

"*77. La Corte ritiene che emerga chiaramente dal fascicolo del ricorrente che fosse stato informato del divieto di utilizzo di internet per fini personali come emerge dai regolamenti interni del suo datore di lavoro … Tuttavia, non è così chiaro che sia stato informato prima del monitoraggio delle sue comunicazioni che una tale operazione di monitoraggio avrebbe avuto luogo … i giudici nazionali hanno omesso di accertare se il ricorrente fosse stato informato dell'operazione di monitoraggio prima della data in cui è iniziato*";

"*135. Non risulta neppure che i giudici nazionali abbiano effettuato una sufficiente valutazione se vi fossero motivi legittimi per giustificare il monitoraggio delle comunicazioni del ricorrente … la questione era stata toccata dalla Corte della contea, che aveva citato la necessità di evitare danneggiamenti al sistema IT aziendale, la responsabilità della società in caso di attività illegali nel cyberspazio e la divulgazione di segreti commerciali. Tuttavia, a parere della Corte, questi esempi possono essere visti solo come teorici, poiché non vi era alcuna indicazione che la ricorrente avesse in realtà esposto l'azienda a qualsiasi di tali rischi*".

La CEDU ha individuato espressamente i criteri che devono guidare i giudici nazionali nel valutare se una determinata misura di controllo sia proporzionata all'obiettivo perseguito e se il dipendente interessato sia tutelato contro interferenze arbitrarie nella sua sfera personale.

A tale riguardo, i giudici devono valutare se al dipendente è stata comunicata o meno la possibilità che il datore di lavoro possa monitorare la sua attività e come vengono attuate tali misure; quale sia l'estensione del controllo da parte del datore di lavoro e il grado di intrusione nella privacy del dipendente; se il datore di lavoro abbia fornito motivazioni legittime per giustificare il monitoraggio; se sia possibile istituire un sistema di monitoraggio basato su metodi e misure meno intrusivi; quali siano le conseguenze del monitoraggio per il lavoratore subordinato e quale l'uso da parte del datore di lavoro dei risultati dell'operazione di monitoraggio; se siano state predisposte adeguate misure di salvaguardia in favore del lavoratore.

Opinion 2/2017 del Comitato dei Garanti Privacy

Qualche mese prima della decisione della Grande Camera di cui sopra, i Garanti Privacy europei, riuniti nel Gruppo di lavoro "Articolo 29" (WP29), con la Opinion n. 2/2017 dell'8.6.2017 si sono pronunciati in merito al trattamento dei dati dei lavoratori nei luoghi di lavoro anche in relazione alle novità introdotte dal Regolamento UE 2016/679 in vigore dal maggio 2018 (integrando quanto già previsto con l'Opinion n. 8/2001 "Parere sul trattamento di dati personali nell'ambito dei rapporti di lavoro" e con il "Documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sul luogo di lavoro" del 2002).

In particolare il Gruppo, da un lato, muove dalla constatazione che il datore di lavoro può disporre di variegate forme di vigilanza (es. controllo della posta elettronica, sorveglianza dell'accesso ad Internet) che con le nuove tecnologie si sono ulteriormente amplificate dando vita a nuove implicazioni giuridiche in termini di protezione dei dati personali.

Dall'altro lato, i Garanti europei ribadiscono la legittima aspettativa di riservatezza che deve essere riconosciuta al lavoratore, rispetto alla quale devono essere valutati i diritti e gli interessi legittimi del datore di lavoro.

In tale prospettiva di tutela rafforzata, innanzitutto il WP29 esclude quale base giuridica del trattamento dei dati personali dei lavoratori il mero consenso di quest'ultimi posto che, a causa del rapporto di "dipendenza" nei confronti del datore di lavoro, potrebbe ritenersi non liberamente prestato né liberamente revocabile.

Rappresenta, invece, condizione di liceità del trattamento (più decisiva dell'ottenimento del consenso)

il rispetto di quanto previsto dall'art. 6 GDPR: "*Il trattamento è lecito solo se e nella misura in cui ... è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiede la protezione dei dati personali*".

Con riferimento all'interesse legittimo del datore di lavoro, il WP29 impone di valutare preventivamente se il trattamento da porre in essere sia necessario e proporzionato per il perseguimento di una finalità legittima, nonché di adottare misure di sicurezza volte a bilanciare tale finalità con i diritti e le libertà fondamentali dei lavoratori.

Il Gruppo ha sottolineato, in particolare, che ogni lavoratore deve innanzitutto essere adeguatamente informato sulle modalità di trattamento dei dati personali in maniera chiara, semplice ed esaustiva, soprattutto quando siano previste forme di controllo.

Il parere individua ipotesi tipiche di trattamento di dati personali dei lavoratori che possono presentare dei rischi per i diritti e le libertà fondamentali di quest'ultimi e tra queste proprio il monitoraggio della strumentazione informatica dei lavoratori (es. email ricevute e inviate, siti web visitati, telefonate effettuate).

In particolare è sollecitata l'adozione di specifiche soluzioni volte a prevenire il ricorso ad accessi "successivi" ai dati dei lavoratori (esempio la cronologia web o la casella di posta elettronica) e l'adozione di misure quali la predisposizione di un elenco di siti in cui la navigazione è vietata, la previsione di caselle di posta personali, l'individuazione di aree di memoria private, quali l'archivio fotografico.

La posizione del Garante nazionale

Anticipando sia la giurisprudenza dei giudici di Strasburgo che il Comitato WP29, il Garante italiano ha adottato già nel 2007 le "Linee guida del Garante per posta elettronica e internet" (delib. n. 13 del 1.3.2007) che prevedono le misure "*necessarie e opportune per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete internet*".

Tali linee guida prevedono l'obbligo per il datore di lavoro di fornire indicazioni chiare ai propri lavoratori sull'utilizzo consentito degli strumenti di lavoro e dei possibili controlli.

In assenza di tali indicazioni i lavoratori sono legittimati a ritenere tollerato l'utilizzo di strumenti quali internet e la posta elettronica anche per scopi personali, nel rispetto della propria riservatezza:

«*3. Controllo e correttezza nel trattamento.*

3.1. (...) Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli.

(...) 3.2 In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall´art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

(...) All´onere del datore di lavoro di prefigurare e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell´art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2.

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli»

Peraltro, in tale documento il Garante sgombra il campo dall'equivoco circa la prospettata "impersonalità" della cronologia internet estratta da pc.

Partendo dalla constatazione che la semplice elencazione degli indirizzi dei siti visitati può rivelare dati delicatissimi della persona quali convinzioni religiose, opinioni politiche, appartenenza a partiti, sindacati o associazioni, stato di salute, indicazioni sulla vita sessuale, il Garante impone al datore di lavoro «*l'adozione di misure di tipo tecnologico*» atte a garantire il «*rispetto della navigazione in internet*» anche nel senso di «*precludere l'immediata identificazione degli utenti*» oltre al divieto di «*conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza*» (par. 2, lett. c, della parte dispositiva).

In tema di trattamento dei dati connessi al rapporto di lavoro e controllo a distanza, il Garante ha deciso in più occasioni ritenendo determinante della illiceità della condotta datoriale l'assenza di informativa ovvero la sua inadeguatezza.

Viene in rilievo sul punto il Provvedimento n. 307

del 18.10.2012 (doc. web 2149222) relativo a un licenziamento per giusta sulla base delle informazioni assunte dal datore di lavoro in occasione dell'esecuzione delle operazioni di back up del portatile aziendale concesso in uso al lavoratore. Il Garante ha sanzionato il datore di lavoro per non aver "*fornito una idonea informativa in ordine al trattamento dei dati personali connesso ad eventuali attività di verifica e controllo effettuate dalla società stessa sui PC concessi in uso ai dipendenti*".

Ancora, si segnala il Provvedimento n. 53 del 1.2.2018 (doc. web n. 8159221) relativo a un licenziamento disciplinare fondato sul contenuto di comunicazioni email rinvenute dal datore di lavoro in occasione di un accesso tramite server aziendale alla casella di posta elettronica aziendale, individualizzata con nome e cognome. Il Garante, accertato che "non risulta che la società abbia informato il reclamante - e gli altri dipendenti – circa le modalità e finalità della descritta attività di raccolta e conservazione dei dati relativi all'utilizzo della posta elettronica", ha ritenuto "in contrasto con la disciplina di settore in materia di controlli a distanza (cfr. art. 11 Codice e art. 4 S.L.) ... la raccolta sistematica delle comunicazioni in transito sugli account aziendali dei dipendenti in servizio e cessati, la loro memorizzazione per un periodo non predeterminato e la possibilità di accedervi per finalità indicate in astratto e in termini generali – quali la difesa in giudizio o il perseguimento di un legittimo interesse".

Infine, si segnala il Provvedimento n. 216 del 4.12.2019 (doc. web n. 9215890) relativo alla mancata disattivazione dell'account di posta elettronica di tipo individualizzato per un ampio periodo di tempo, con contestuale accesso ai messaggi ivi pervenuti, successivamente alla cessazione del rapporto di lavoro. Il Garante ha ritenuto la illiceità della condotta aziendale anche alla luce della "assenza di una policy aziendale resa nota ai dipendenti al riguardo".

Con il Provvedimento n. 65/2020 il Garante, quindi, ha confermato il proprio orientamento in merito alla imprescindibilità della informazione preventiva all'interessato in ordine alle caratteristiche essenziali del trattamento effettuato.

Non solo. Con espresso riferimento alla formulazione del regolamento aziendale oggetto della pronuncia, nel senso che "È proibita la navigazione in internet per motivi diversi da quelli funzionali all'attività lavorativa stessa; ai fini della tutela del patrimonio aziendale con regolarità si provvederà a verificare i collegamenti alla rete internet su ogni client nel rispetto delle norme sulla privacy", il Garante ha ritenuto "non conforme ai principi di liceità e proporzionalità" il mero riferimento a "controlli "regolari" (senza specificare le modalità)".

La giurisprudenza italiana tra violazioni disciplinari e oneri datoriali

Al rigore del Garante (in linea, come ricordato, tanto con la giurisprudenza CEDU quanto con le indicazioni dei Garanti europei) non si è conformata invece la giurisprudenza dei nostri giudici di merito e della cassazione.

Per stare a quest'ultima è già stata criticata su questa rivista la sentenza n. 3133 del 1° febbraio 2019 (*Guida al Lavoro* n. 7/2019) che ha riguardato il caso delle conseguenze disciplinari derivanti dall'uso di internet per motivi personali, durante l'orario di lavoro e mediante utilizzo dei dispositivi aziendali.

Precisamente, si tratta di una decisione di conferma della legittimità del licenziamento per giusta causa irrogato a una lavoratrice a seguito di indagine condotta sulla cronologia internet del pc in uso presso lo studio professionale nel quale era impiegata.

In particolare, non convince l'asserita legittimità delle concrete modalità di accertamento della violazione utilizzate dal datore di lavoro che ha avuto accesso alla cronologia degli accessi internet senza aver prima posto in essere precisi adempimenti richiesti, abbiamo visto, dalla normativa a tutela della privacy.

Nel contesto normativo sintetizzato ai paragrafi precedenti, la quantità degli accessi a internet a fini personali non è un elemento di per sé determinante ai fini della legittimità o meno del licenziamento (come peraltro dimostrano i precedenti giurisprudenziali che in situazioni del tutto analoghe a quella oggetto di Cass. n. 3133/2019 sono giunti a risultati opposti[3]) quanto piuttosto la forma e la conoscibilità degli accertamenti condotti dal datore di lavoro.

3. *Si vedano in proposito:*
- Cass. 22353/2015 dichiara illegittimo il licenziamento per giusta causa di un lavoratore per uso illegittimo del PC aziendale, delle reti informatiche aziendali e della casella di posta elettronica, se il datore di lavoro non prova un danno ulteriore. Nello specifico, non era risultato in giudizio che la navigazione in internet del dipendente avesse determinato una significativa sottrazione di tempo all'attività di lavoro.

In tema è intervenuta la recentissima Cassazione n. 4871 del 24 febbraio 2020 relativa al licenziamento disciplinare di un dipendente bancario che ha eseguito interrogazioni sui conti correnti dei clienti, non sostenute da ragioni di servizio, violandone la privacy.

La Cassazione, confermando quanto stabilito dalla Corte d'appello, afferma che – ai sensi dell'art. 4, comma 3, L. 300/1970, come sostituito dall'art. 23 D.Lgs. n. 151/2015 – il datore di lavoro può utilizzare per tutti i fini connessi al rapporto di lavoro, le informazioni raccolte mediante le apparecchiature utilizzate dai dipendenti, se sussistono i requisiti espressi dai commi 1 e 2 del predetto art. 4 dello Statuto dei Lavoratori.

Per i Giudici di legittimità, condizione essenziale, a tal fine, è che venga fornita idonea notizia ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli c.d. difensivi, nel rispetto di quanto disposto dal Codice della Privacy.

Onere questo che, secondo la sentenza, nel caso di specie è stato "assolto dalla Banca nei confronti della generalità dei propri dipendenti, indipendentemente dalla loro qualifica, attività o funzione, stabile o temporanea, e ciò in ragione della stretta ed essenziale inerenza all'attività bancaria della tutela della riservatezza della clientela e del rischio diffuso di indebiti accessi alle relative posizioni tramite l'utilizzo dei sistemi informatici".

Su tali presupposti, la Suprema Corte ha rigettato il ricorso proposto dalla lavoratrice, confermando la legittimità del licenziamento irrogatole. ●

- Cass. 26397/2013 conferma l'illegittimità del licenziamento di un lavoratore che aveva scaricato sul pc aziendale alcuni file e poi usato un programma di file sharing per condividerli con amici in quanto il CCNL di riferimento prevedeva per questo tipo di comportamento una sanzione conservativa.

- Trib. Torino 18.9.2018 n. 1664 illegittimità di un licenziamento comminato ad un lavoratore, accusato, a seguito di controlli effettuati sul computer aziendale, di aver utilizzato il suo pc aziendale per fini personali ed estranei all'oggetto della prestazione lavorativa. Il giudice precisa che la soluzione della controversia è in ogni caso connessa all'assolvimento dell'onere dell'informativa di cui all'articolo 4 comma 3 dello Statuto dei Lavoratori.

Secondo il giudice di merito, infatti, il datore di lavoro non avrebbe fornito un'adeguata informativa, in particolare con riferimento alle modalità di effettuazione dei controlli datoriali. Ciò si è pertanto rivelato preclusivo non solo dell'utilizzo delle informazioni raccolte attraverso gli strumenti di lavoro affidati al dipendente, ma anche di quelle raccolte attraverso l'impiego di strumenti tecnologici, come il proxy di navigazione, dai quali derivi la possibilità di controllo a distanza dell'attività lavorativa.

- Trib. Firenze 7.1.2008 n. 1218 dichiara illegittimo il licenziamento del dipendente che ha dedicato circa 59 minuti giornalieri ad internet. L'annullamento del licenziamento si è basato anche sul fatto che il datore di lavoro aveva sempre consentito tali accessi seppur nei limiti della ragionevolezza.

In senso contrario si vedano invece:

- Trib. Bari 10.6.2019 n. 2636 secondo la quale costituisce grave illecito disciplinare il comportamento di un dipendente che - oltre ad installare indebitamente un profilo Facebook sul telefono aziendale nella propria esclusiva disponibilita e a impiegare tale dispositivo per intrattenere frequenti e numerose conversazioni private durante le ore di lavoro - riveli, per il tramite del predetto dispositivo, informazioni e notizie riservate afferenti all'impresa ad aziende concorrenti dirette.

- Cass. 13266/2018 non ritiene rientrante nel campo di applicazione dell'art. 4 dello Statuto le verifiche effettuate tramite il tracciamento informatico degli accessi ove dirette ad accertare comportamenti illeciti del dipendente dai quali possano derivare effetti negativi sul patrimonio aziendale e sull'immagine dell'impresa. In tal caso, l'assenza di una policy aziendale non rileva poiché l'addebito disciplinare contestato al lavoratore attiene alla violazione dei suoi doveri fondamentali di diligenza nello svolgimento dei propri compiti.

- Cass. 14862/2017 ha confermato la legittimità del licenziamento irrogato nei confronti di un dipendente che, per un totale di 45 ore, aveva utilizzato la connessione internet aziendale per fini personali, sottraendo buona parte del proprio tempo-lavoro allo svolgimento delle mansioni assegnateli.

- Cass. 17859/2014 dichiara legittimo il licenziamento disciplinare del dipendente che, sul computer aziendale, abbia installato un programma di "file-sharing" ed uno per l'accesso alla email personale, effettuando il "download" di foto e filmati pornografici qualora il codice disciplinare affisso nella bacheca aziendale vieti l'accesso alla rete internet e l'utilizzo della posta elettronica per scopi personali.