Seminario del 17 Gennaio 2022

LAVORO IN PRESENZA, LAVORO AGILE: IL CONFINE TRA DIRITTO ALLA RISERVATEZZA E POTERE DI CONTROLLO

A cura del Dipartimento Giuridico Fisac-CGIL

Interventi di:
Enrica Crimi
Carlo Mancino
Alberto Massaia
Avv. Juri Monducci
Alessandra Orlando

Indice

FOCUS SUL SETTORE, REGOLE E CRITICITA'

1. Introduzione ai temi in trattazione

In questo seminario ci occuperemo di approfondire per quanto possibile, nel tempo a nostra disposizione, gli aspetti salienti del delicatissimo, estremamente dibattuto e intricato tema del confine tra il **diritto alla riservatezza** e il **potere di controllo** sul luogo di lavoro, focalizzando la nostra attenzione su quanto accade nel settore del credito e delle assicurazioni.

La trattazione si innesterà nel più generale dibattito sui confini spesso effimeri della dicotomia tra l'esigenza di protezione e sicurezza (del patrimonio nel nostro caso, del datore di lavoro. Dove l'esigenza di protezione copre sia beni materiali dell'azienda -> strumenti di lavoro; sia quelli che si possono definire beni immateriali -> diritto a ricevere adeguata prestazione del lavoratore) e la garanzia delle libertà individuali (del lavoratore).

Quando ci approcciamo a tali approfondimenti, è bene ricordare che stiamo parlando di temi complessi, intricati e in rapida e continua evoluzione, il cui punto di equilibrio è spesso influenzato da fasi storiche, rapporti di forza, fattori esogeni non controllabili dagli attori.

Basti pensare, per restare solo a quanto accaduto negli ultimi anni:

- alle piccole-grandi rivoluzioni normative di cui siamo stati testimoni con la riforma approvata nel 2015 avente ad oggetto l'Art. 4 della legge 300, che ha radicalmente modificato il perimetro e l'ampiezza di applicazione dei controlli a distanza;
- alle evoluzioni organizzative conseguenti allo sviluppo e alla diffusione degli strumenti informatici hardware e software (on line banking, contact center, device per fornire la prestazione lavorativa...);
- alle profonde quanto impreviste mutazioni delle condizioni lavorative dovute allo scoppiare della pandemia che stiamo ancora affrontando.

Senza dubbio, vista la fluidità degli argomenti in trattazione, in futuro ci troveremo ad affrontare ulteriori, nuovi e (magari) oggi inimmaginabili cambiamenti.

Un altro tema caldo su cui ci soffermeremo, legato a quanto sopra e fortemente accentuato dalle evoluzioni organizzative, è quello del **diritto alla disconnessione**.
Tutela della privacy e diritto alla disconnessione sono infatti due facce della stessa medaglia e costituiscono una limitazione del potere di controllo da parte dell'impresa.
Il problema del diritto alla disconnessione è certamente configurabile anche nel lavoro in presenza, ma emerge in maniera netta e incisiva nel lavoro agile e con l'utilizzo di nuovi device e strumenti di lavoro "smart".

Qui si inserisce una inclinazione derivante dalla specificità del settore bancario che, come tutto - o molto - di quanto rientra nel settore dei servizi, trova un suo punto di attenzione nell'oggetto stesso della prestazione che spesso, non essendo "fisicamente misurabile" (ad esempio, come in una linea di produzione industriale) è facilmente espletabile in luoghi diversi dal posto di lavoro, soprattutto con l'evoluzione dei sistemi informatici e la diffusione delle device aziendali concesse ai dipendenti.

2. Evoluzione dell'organizzazione del lavoro nel settore bancario e assicurativo

Negli ultimi 2 anni abbiamo assistito a un profondo cambiamento del modo in cui può essere fornita la prestazione lavorativa e il tema del lavoro agile ha assunto importanza primaria del settore bancario, dopo anni in cui il suo incremento è stato lento e incerto, valutato forse con eccessiva prudenza dall'intero settore, specchio di un retaggio culturale diffuso per cui la presenza fisica del cosiddetto "padrone" nel luogo in cui si svolge la prestazione garantisce l'impegno del dipendente.

Complice la pandemia, il ricorso a tale tipologia di lavoro ha avuto un rapido e inaspettato incremento creando, a fronte degli evidenti vantaggi in periodi di lockdown più o meno rigidi, anche non pochi problemi sotto diversi aspetti.

Possiamo dire che la pandemia ha svolto un ruolo di spartiacque del processo di diffusione del lavoro a distanza.

Nel settore bancario (ma non solo, evidentemente) si potrebbe parlare di un "Ante Pandemia" e "Post Pandemia".

Per comprendere la dimensione del fenomeno, basti pensare che nel nostro settore, rientrante tra i servizi essenziali regolamentati dalla legge 146/90, si è passati (statistica dei primi 6 gruppi):

- Dal 4,9% di personale in smartworking nel 2019 al 51,7% del marzo 2020, da una media di 8.500 a 90.000 persone in sw al giorno.
- In rete si è passati dallo 0,2% al 27,3% (incremento del 13.650%!).
- Negli uffici interni e nelle sedi dal 18% al 84,5% del personale in sw durante il lockdown.

Certo, sono numeri di un periodo particolarmente complesso e, speriamo tutti, irripetibile. Ma è chiaro a tutti che ha dato la stura alla diffusione del lavoro a distanza e con ogni probabilità non si tornerà più a numeri ante pandemia.

Tutto ciò, ha avuto un impatto enorme sull'organizzazione del lavoro, sui sistemi IT, e - per quanto riguarda la materia di nostro interesse - sugli strumenti, sui controlli a distanza e sul diritto alla disconnessione.

3. Il rischio di commistione tra lavoro e vita privata

Le nuove modalità di fornire la prestazione lavorativa, i confini sempre più indefiniti tra lavoro e vita privata, i tempi che si intrecciano (sera, dopocena...), i luoghi dove viene svolta l'attività lavorativa che finiscono per coincidere con i luoghi della vita privata (il divano di casa, il tavolo della

cucina...), gli strumenti hardware (smartphone, PC) e software (gruppi whatsapp tra colleghi dove girano comunicazioni lavorative di ogni tipo, social) possono provocare anche una percezione rischiosa di quanto si fa in un dato momento.

Sto agendo nella sfera della mia attività lavorativa o nella sfera privata? Dove si pone la linea di demarcazione? Come faccio a distinguerlo?

Il rischio è sempre più quello di vivere, utilizzando le parole del Prof. Zagrebelsky, in un "eterno presente" in cui i contorni della prestazione lavorativa sfumano in un unico indefinibile, rischiando addirittura di confondere il confine storicamente ben delimitato tra i concetti di **obbligazione di mezzi** e di **obbligazione di risultato**.

4. Panoramica della situazione nel settore

Sulla base di quanto detto sopra, dobbiamo rilevare che lo stato dell'arte nel settore del credito è oggi molto eterogeneo, con accordi stipulati all'interno dei Gruppi che si presentano vari e variegati, con tempi di sottoscrizione che vanno indietro di anni, in alcuni casi precedenti al jobs act.

Il tutto in un quadro in veloce (e inaspettata) evoluzione.

LAVORO IN PRESENZA E LAVORO AGILE:
IL CONFINE FRA DIRITTO ALLA RISERVATEZZA E POTERE DI CONTROLLO

Una premessa "filosofica"

Spesso corsi, seminari e presentazione si aprono con il frammento di un film o con una canzone o qualcosa di simile.

Invece, visto che l'argomento del mio intervento è piuttosto impegnativo, per entrare in argomento vi mostrerò un disegno architettonico e due

fotografie di un edificio ponendovi l'indovinello se riconoscete l'edificio o se almeno riconoscete di quale tipologia di edificio si tratti.

Detto così sembra difficilissimo, ma quando ne ho parlato con una mia amica e compagna di sindacato, questa mi ha detto che l'aveva già visto anni fa in un corso di formazione: ma non si ricordava se fosse un corso della CGIL oppure della banca. Ahimé…

Un bel gioco dura poco: ecco il disegno, inizio a chiacchierare e a fornirvi qualche elemento e nel frattempo farete appello alla vostra memoria o al vostro intuito.

- Il progetto risale al 1791 ed è opera di un filosofo e giurista oltreché architetto dilettante.
- Raffigura un'architettura neoclassica di certo non ateniese ma assai spartana e vista l'epoca ha un affascinante nome greco antico.
- Se i progetti di Nicholas Ledoux sono espressione di un neoclassicismo utopistico, questo disegno è l'esatto contrario, è di un neoclassicismo distopico, frutto di un'intelligenza tanto acuta quanto perversa.
- Si tratta di un edificio assolutamente avveniristico e utilitaristico e che non ha nulla di monumentale.
- La planimetria è fondamentale nella filosofia di quest'edificio.

- Questa è una fotografia di un edificio costruito nel 1931 a Cuba su un progetto che riprendeva il disegno del 1791: è in disuso da parecchi decenni ma è ancora visitabile.

- Infine, questa è una fotografia di un altro edificio del 1925 a Stateville negli Stati Uniti che riprende il medesimo progetto e l'immagine è chiarissima per capire di che cosa si tratta: è un carcere.

Il progetto è quello del Panopticon – in greco antico: “vedo tutto” – ed è un’ideazione di Jeremy Bentham.
La caratteristica fondamentale è la planimetria circolare: le celle dei carcerati sono disposte lungo la circonferenza e sono chiuse da una cancellata in ferro che lascia libera la visuale. Al centro s’innalza una torre dove è collocato un solo carceriere che attraverso le feritoie della torre può osservare tutti i carcerati senza essere visto.

L’idea di Bentham era quella di inculcare nei carcerati l’idea che il carceriere poteva spiarli in ogni momento, ma ogni singolo carcerato non poteva sapere in quale momento era spiato, con il risultato che si sentiva costantemente spiato anche quando non lo era.
Oltre a questo, i carcerati dovevano lavorare nelle loro celle, in modo che il carcere fosse redditizio. Secondo Bentham questo sistema avrebbe reso i carcerati docili e remissivi nei confronti dei carcerieri e dell’autorità in generale.

Riassumendo: vedere senza essere visti, controllare tutto e tutti stando sempre nell’ombra, creare un’atmosfera di timore reverenziale e un’obbedienza incondizionata. Sono concetti che usualmente associamo agli stati totalitari del XX secolo, ma purtroppo si perdono nei secoli e temo che oggi siano più forti che mai.
Michel Foucault – il filosofo che si dedicò soprattutto ad analizzare i rapporti di potere - scrisse un saggio *Sorvegliare e punire*, in cui usa addirittura il termine “panoptismo” per indicare un potere visibile ma inverificabile, sul modello della torre del carceriere ideata da Bentham, ben visibile a tutti i carcerati che non possono mai sapere se il carceriere li osserva o no: il controllo occulto come espressione del potere e il carcere come metafora della società, non necessariamente dittatoriale, sia chiaro.

Bene dopo questa premessa filosofica sufficientemente inquietante e distopica, passiamo a una premessa seria di carattere metodologico.

1. Premessa

Gli argomenti del controllo a distanza e della tutela della privacy sono non soltanto complessi, ma anche evanescenti e proteiformi - come certi mostri marini della mitologia antica – e si espandono a toccare una ridda di altri argomenti.

Così, la tutela della privacy del lavoratore è una limitazione del potere di controllo da parte dell'impresa; a loro volta il potere di controllo e il diritto alla disconnessione sono due facce della stessa medaglia, in quanto se il lavoratore è disconnesso esce dalla sfera di controllo dell'impresa.

L'impresa esercita il potere di controllo sia nel caso di lavoro in presenza che nel caso di lavoro agile, ma il controllo è più pervasivo nel secondo caso, come contrappeso alla mancanza di un controllo "visivo" da parte dei superiori gerarchici.

Il diritto alla disconnessione è configurabile anche nel lavoro in presenza, ma emerge in maniera netta nel lavoro agile; non a caso è enunciato nella legge n. 81/2017 nel capo II che tratta per l'appunto del lavoro agile.

Inoltre, la risoluzione del Parlamento Europeo del 21 gennaio 2021 - che affronta in modo specifico il diritto alla disconnessione - stabilisce un parallelo con l'orario di lavoro. Si tratta di un parallelo che a prima vista può sembrare incoerente e contraddittorio, se si considera che il lavoro agile sembra superare il concetto di orario di lavoro, rendendo reali certe tesi politiche, che in Italia furono sostenute ad esempio il ministro Poletti al tempo del governo Letta. In realtà, il parallelo ha una precisa logica, se si considera il concreto rischio che il lavoro agile possa debordare sino a rendere ogni giornata una commistione indistinta di spazi e tempi di lavoro

e di vita privata, in cui i concetti di orario di lavoro e anche di giorni lavorativi e giorni festivi diventano evanescenti.

E infine, la rilevanza o meno dell'orario è uno degli elementi distintivi fra lavoro dipendente oppure autonomo, al pari dei concetti di obbligazione di mezzi e di obbligazione di risultato.

A questo punto, appare evidente che ci troviamo davanti a una ridda di argomenti tutti legati da correlazioni logiche:

- controllo a distanza;
- tutela della privacy;
- diritto alla disconnessione;
- lavoro in presenza e lavoro agile;
- orario di lavoro;
- obbligazione di mezzi e obbligazione di risultato;
- lavoro dipendente e lavoro autonomo.

Ovviamente non sarà possibile affrontare tutti questi temi in forma esaustiva e completa, l'esposizione sarà focalizzata sui due temi principali, ma sarà necessario evidenziare le numerose correlazioni con altre tematiche per cogliere pienamente la complessità del controllo a distanza e della tutela della privacy.

Ciò comporterà in primo luogo l'esame delle normative di legge nazionale e in alcuni casi sovranazionali, quindi l'esame della giurisprudenza. Questo per il motivo gli accordi sindacali sull'argomento di oggi e che rappresentano un impegnativo banco di prova per la contrattazione sindacale, dovranno basarsi sulle tutele di legge così come interpretate dalla giurisprudenza e da queste svilupparsi per giungere a un accordo che sia il più tutelante possibile, con gli ovvi limiti derivanti dai rapporti di forza e dalle mediazioni.

2. La normativa di legge sul controllo a distanza dei lavoratori: l'art. 4 della legge n. 300/1970 e le modifiche apportate dal decreto legislativo n. 151/2015.

La normativa sul controllo a distanza dei lavoratori, contenuta nell'art. 4 della legge n.300/1970 era chiara, lineare ed esprimeva principi di portata assolutamente generale; quest'ultima caratteristica la rendeva sempre attuale; la presunta obsolescenza della legge è stata solo un alibi del tutto infondato per giustificare un intervento di controriforma a favore delle imprese.

In primo luogo, l'art 4 della legge del 1970 si apriva con tale principio:

"È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori."

Il termine "altre apparecchiature" era assolutamente generico e ricomprendeva qualunque ritrovato tecnologico sconosciuto nel 1970 e diventato attuale mezzo secolo dopo: l'importante non era lo strumento in sé ma la finalità del controllo e il controllo a distanza era semplicemente vietato.

Quindi, l'articolo continuava con la precisazione che le apparecchiature di controllo richieste da esigenze organizzative e produttive oppure dalla sicurezza del lavoro, ma dai quali derivasse la possibilità di controllo a distanza dell'attività dei lavoratori, potessero essere installate soltanto previo accordo sindacale, oppure - in mancanza di accordo – con autorizzazione dell'Ispettorato del lavoro.

La giurisprudenza della Corte di Cassazione, in relazione alla norma così come enunciata nel testo originario del 1970, era approdata ad alcuni punti

fermi, cercando di limitare *"le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore (….) sul presupposto che la vigilanza sul lavoro (…) vada mantenuta in una dimensione umana, e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*" (Cassazione, sentenza n. 8250/2000).

Peraltro, la Suprema Corte aveva elaborato il concetto di "controllo difensivo", che non era diretto a verificare l'esatto adempimento delle obbligazioni derivanti dal rapporto di lavoro, bensì a impedire comportamenti illeciti lesivi del patrimonio aziendale. In relazione a tale controllo non sussistevano i vincoli previsti dalla legge n. 300/1970: si trattava a tutti gli effetti di un indebolimento delle tutele a favore dei lavoratori che derivava da un'interpretazione giurisprudenziale limitativa della legge.

Peraltro, il concetto di "patrimonio aziendale" piuttosto che di "beni e interessi aziendali" ha avuto interpretazioni assai oscillanti, che si potevano estendere anche all'onorabilità e reputazione dell'impresa, che poteva essere minacciata da qualunque affermazione ingiuriosa. Analogamente, il concetto di "comportamento illecito" poteva riguardare qualunque comportamento che influisse negativamente sulla prestazione lavorativa.

Il decreto legislativo n. 151/2015, art. 23, ha attuato una radicale riscrittura dell'art. 4 della legge n. 300/1970 introducendo così la nuova disciplina del controllo a distanza dei lavoratori oggi in vigore.

In prima battuta, la nuova normativa riprende il principio generale espresso dalla legge del 1970, con poche modifiche. Infatti, il primo comma dell'art. 4 – come riformulato nel 2015 - riguardo agli strumenti dai quali derivi la

possibilità di controllo a distanza dell'attività dei lavoratori, stabilisce che possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Inoltre, per tali installazioni resta necessario l'accordo sindacale oppure l'autorizzazione dell'ispettorato del lavoro. La principale modifica è rappresentata dall'aggiunta della tutela del patrimonio aziendale quale scopo per cui possono essere installate le apparecchiature in questione, facendo sorgere il dubbio del superamento dei "controlli difensivi".

Tuttavia, nel comma 2 dell'art. 4 il decreto del 2015 introduce una deroga amplissima al principio che abbiamo appena citato. La deroga riguarda gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze. La deroga fa venire meno sia i limiti di finalità (organizzative, produttive, sicurezza del lavoro, tutela del patrimonio aziendale), sia la necessità dell'accordo sindacale o dell'autorizzazione amministrativa.

Dalla mera lettura testuale, la nuova legge attribuisce al datore di lavoro un potere amplissimo di controllo su computer (e di conseguenza possono essere controllate gli accessi a internet e le e-mail), telefoni fissi e portatili, tablet, tutti strumenti diffusamente utilizzati in qualunque realtà di lavoro impiegatizio e non solo. I concetti di "strumento di controllo" e di "strumento di lavoro" si sovrappongono, con il risultato che il controllo può raggiungere livelli estremamente pervasivi. Inoltre, la previsione di strumenti di controllo a difesa del patrimonio aziendale – come elaborata dalla giurisprudenza passa in secondo piano rispetto al controllo degli strumenti di lavoro.

Inoltre, il decreto del 2015 prevede esplicitamente che i dati raccolti possano essere utilizzati a tutti i fini connessi al rapporto di lavoro: in altre parole anche in ordine alle sanzioni disciplinari, che potrebbero arrivare al licenziamento. È di tutta evidenza quanto possa essere temibile il

combinato disposto di tale potere di controllo e della pressoché completa liberalizzazione dei licenziamenti attuata con il decreto legislativo n. 23/2015, sempre compreso nel pacchetto normativo del “Jobs act”.

L’unica tutela per i lavoratori è prevista nel comma 3 ed è rappresentata dall’onere per il datore di lavoro di dare avviso delle modalità d’impiego degli strumenti e delle modalità di controllo, con un generico richiamo alla normativa sul trattamento dei dati sensibili di cui al decreto legislativo n. 196/2003.

Appare evidente il rovesciamento d’impostazione operato dal decreto del 2015 rispetto alla legge del 1970; sbiadisce anche la distinzione giurisprudenziale fra i controlli diretti a verificare l'esatto adempimento delle attività lavorative ed i controlli diretti a tutelare i beni aziendali o a impedire comportamenti illeciti.

3. La legislazione del 2015 interpretate dalla giurisprudenza.

La normativa introdotta nel 2015 è giunta al vaglio della magistratura del lavoro, soprattutto della corti merito, anche se è ancora presto per ritenere che la giurisprudenza sia consolidata.

Segnaliamo le seguenti sentenze:

- Corte d’Appello di Perugia 30 settembre 2019;
- Tribunale di Pescara 25 ottobre 2017;
- Tribunale di Padova 22 gennaio 2018;
- Tribunale di Roma 13 giugno 2018;
- Tribunale di Venezia 23 luglio 2020;
- Corte di Cassazione n. 25731/2021;
- Corte di Cassazione n. 25732/2021;
- Corte di Cassazione n. 32760/2021.

Di particolare interesse è la sintesi esposta nella sentenza dal Tribunale di Roma nei termini di seguito riportati.

"Il lavoratore può ben essere controllato con mezzi a distanza, ma alle seguenti cumulative condizioni:
a) l'impianto deve essere stato previamente autorizzato con accordo sindacale o dall' INL;
b) l'impianto deve avere una o più delle finalità (diverse da quelle di controllare i lavoratori) previste dal primo comma dell'art.4;
c) il datore deve aver previamente informato il lavoratore che l'impianto è stato installato, e che vi si potranno esperire controlli (comma 3);
d) il controllo deve essere esperito in conformità al Codice della privacy, il che comporta essenzialmente che esso va fatto secondo i principi di trasparenza, scopo legittimo e determinato, non invasività, ricavabili dall'art. 11 del D.lgs. 196/2003 e s.m..
Le regole sub a) e b), che dettano, rimodulandolo, il regime procedurale autorizzatorio, non valgono per gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", quali ad esempio il computer e la e-mail aziendale.
Le regole sub c) e d) valgono invece sempre, alla sola condizione che si tratti di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori".

Inoltre, per quanto riguarda la modalità dell'informativa la sentenza del Tribunale di Venezia ha stabilito che non è sufficiente la circostanza che i lavoratori siano a conoscenza della presenza di telecamere, in quanto manca l'informazione circa le modalità d'uso dei dati acquisiti e l'autorizzazione a effettuare controlli sulla prestazione lavorativa.

Sullo stesso argomento, la sentenza della Corte d'Appello di Perugia ha ritenuto insufficiente un'informativa tramite cartelli che segnalano la presenza degli impianti audiovisivi e tramite la messa a disposizione

dell'informativa stessa nell'ufficio del personale, in una guardiola e nell'intranet aziendale: *"l'informazione deve esser data al lavoratore e non soltanto messa sulla carta a sua disposizione"*.

La sentenza della Corte di Cassazione n. 25731/2021 è più sfaccettata, ma le conclusioni in diritto sono simili a quelle delle sentenze già citate. La causa riguardava il licenziamento di una lavoratrice motivato da uno scambio di corrispondenza su una chat aziendale avente contenuto offensivo nei confronti di altri colleghi; tale fatto era emerso a seguito di un controllo effettuato da tecnici informatici per verificare se in occasione della chiusura della chat vi fossero dati aziendali da conservare.
La Suprema Corte ha confermato la precedente sentenza della Corte d'Appello di Milano accogliendone le ragioni. In particolare, ha considerato il licenziamento illegittimo con conseguente diritto alla reintegra in quanto basato su materiale ricavato in violazione del d.lgs. n.151/2015 art. 23 in quanto la società aveva dato la comunicazione dei controlli quando i controlli stessi erano stati già eseguiti, senza la necessaria e tempestiva informazione ai dipendenti.
Oltre a questo aspetto formale, la sentenza ha accertato che l'accesso alla chat era possibile solo con l'uso di una password e che i messaggi inviati potevano essere letti solo dai destinatari: pertanto la conversazione seppure litigiosa costituiva una forma corrispondenza privata e come tale rientrante nelle previsione dell'art. 15 della Costituzione che tutela la libertà e segretezza delle comunicazioni, con la conseguenza che l'accesso al contenuto delle comunicazioni è precluso agli estranei e non ne è consentita la rivelazione ed utilizzazione.

Dall'esame delle sentenze, emergono almeno due tratti in comune.
1) In tutti i casi si tratta di impugnazioni di licenziamenti e sanzioni disciplinari e tale circostanza è illuminante su quale sia il principale esito della riforma del 2015; pur nella diversità degli elementi in fatto – in alcuni casi oggetto del contendere sono le tradizionali telecamere, in altri

strumenti di controllo più tecnologici - le pronunce approdano ad analoghi principi di diritto.

2) Inoltre, le sentenze citate hanno dichiarato illegittimo l'utilizzo a fini disciplinari dei dati raccolti dal datore di lavoro in quanto in tutti e quattro i casi era mancata l'informativa ai lavoratori: si tratta di un aspetto formale sicuramente importante, tuttavia è probabile che con il passare del tempo le imprese si adeguino a tale prescrizione, rendendo sempre più difficoltosa l'impugnazione delle sanzioni.

Un discorso a parte va fatto per la sentenza della Corte di Cassazione n. 25732/2021 – particolarmente vasta e complessa – che ha affrontato il caso di una lavoratrice licenziata per l'utilizzo scorretto di internet in orario di lavoro e sul computer aziendale.

I fatti contestati erano emersi in quanto il datore di lavoro si trovò nella necessità di svolgere accurati controlli sui computer aziendali causa di un virus che aveva causato seri danni al sistema informatico dell'impresa, criptando cartelle e documenti sull'intero server. Le verifiche avevano accertato che il virus informatico derivava da un sito internet visitato dalla lavoratrice; ulteriori accertamenti avevano fatto emergere che la stessa trascorreva un tempo non giustificato su siti non pertinenti all'attività lavorativa e sulla propria casella di posta elettronica.

La Corte d'Appello di Roma aveva considerato legittimo il licenziamento, ma tale sentenza è stata cassata dalla Suprema Corte.

La sentenza della Cassazione sviluppa una vasta trattazione riguardo ai controlli difensivi, concetto giuridico elaborato dalla giurisprudenza sulla base della legge vigente dal 1970 al 2015, ponendosi in particolare il problema se tali controlli siano stati assorbiti nel nuovo testo del 2015 – che prevede espressamente la finalità della tutela dei beni aziendali – oppure se siano ancora attuali.

La sentenza opera una distinzione fra controlli difensivi "in senso lato" – riguardanti la generalità dei lavoratori - e "in senso stretto" – riguardanti

singoli lavoratori - e considera la seconda fattispecie di tali controlli ancora attuali sotto la normativa vigente. Ritiene altresì che non comportino le tutele – assai esigue – attualmente previste a favore dei lavoratori.
I principi di diritto espressi in questa pronuncia sono stati ripresi da un'altra sentenza della Corte di Cassazione, la n. 34092/2021.

Il carattere dei controlli difensivi "in senso stretto" è indicato nel principio di diritto espresso nella rimessione del caso alla Corte di appello di Roma in diversa composizione:
" *Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni (…) o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali (…) rispetto alle tutele della dignità e riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto."*
In assenza di tali condizioni, l'utilizzo a fini disciplinari dei dati raccolti dal datore di lavoro dovrà avvenire nel rispetto delle tutele previste dalla legge n. 300/1970 come modificata nel 2015.

Occorre aggiungere che in diverse sentenze – anche se la giurisprudenza è oscillante - sono considerati beni e/o interessi aziendali anche la mancata prestazione lavorativa e il decoro dell'impresa; quindi anche un commento contro l'impresa, se giudicato offensivo, può essere oggetto di controlli difensivi.

Infine, particolarmente insidiosa appare la sentenza della Corte di Cassazione n. 32760/2021. Il caso in esame riguardava un lavoratore al quale era stato comminato un giorno di sospensione dal servizio per l'utilizzo scorretto di internet in orario di lavoro e sul computer aziendale. I fatti risalivano al 2011 e quindi erano disciplinati dall'art. 4 della legge n.300/1970 nel testo originario.

Il Tribunale di Roma e poi la Corte d'Appello di Roma avevano dichiarato la sanzione illegittima in quanto il materiale probatorio era stato acquisito effettuando un controllo a distanza dell'attività lavorativa in assenza di un previo accordo sindacale. Inoltre, la società non aveva fornito alcuna prova che i controlli sul computer del dipendente fosse finalizzati alla salvaguardia del patrimonio aziendale.

La Cassazione ha confermato l'illegittimità della sanzione disciplinare confermando la sentenza d'appello e sottolineando che l'illegittimità deriva dal fatto che i fatti oggetto di causa sono precedenti l'entrata in vigore del d.lgs. n. 151/2015.

Tuttavia, la sentenza contiene un "obiter dictum" che come tale è irrilevante per il caso in esame, ma vale come enunciazione di un principio di diritto: *"dopo il cd. Jobs Act, gli elementi raccolti tramite tali strumenti (dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori) possono essere utilizzati anche per verificare la diligenza del dipendente nello svolgimento del proprio lavoro, con tutti i risvolti disciplinari e di altra natura connessi".*

È evidente di come si tratti di un'interpretazione che nella sua genericità rappresenta una larghissima apertura a favore delle imprese, per di più senza neanche fare un cenno ai limiti e alle garanzie indicate invece dal Garante per la protezione dei dati personali.

4. Il diritto alla disconnessione: la legge n. 81/2017 sul lavoro agile e il protocollo 7 dicembre 2021; la risoluzione del Parlamento Europeo del 21 gennaio 2021.

Come già anticipato, il lavoro agile è disciplinato dalla legge n. 81/2017, che – detto per inciso – rappresenta il primo intervento legislativo emanato in Italia che ha regolato tale materia.

In questa sede non esaminiamo la disciplina complessiva di tale tipologia di lavoro, ma ci limitiamo a un richiamo all'art. 19, riguardante l'accordo relativo alla modalità di lavoro agile. In particolare, il comma 1 stabilisce che *"L'accordo individua altresì i tempi di riposo del lavoratore nonché le misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro."*

Tale norma deve essere raccordata con l'art. 18 comma 1 che – fra l'altro - stabilisce quanto segue: *"La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva*."

La legge del 2017 enuncia di certo un principio importante, tuttavia rivela un punto di fragilità nell'assenza di indicazioni anche solo generali su come venga garantita la disconnessione, che sono semplicemente demandate all'accordo – collettivo o individuale – con l'ovvio problema insito nei ben diversi rapporti di forza fra impresa e lavoratore.

Una disciplina più incisiva è stata introdotta dal decreto-legge n. 30/2021 e legge di conversione n. 62/2021, che all'art. 2 comma 1 ter precisa che: *"(…) è riconosciuto al lavoratore che svolge l'attività in modalità agile il diritto alla disconnessione dalle strumentazioni tecnologiche e dalle piattaforme informatiche, nel rispetto degli eventuali accordi sottoscritti dalle parti e fatti salvi eventuali periodi di reperibilità concordati. L'esercizio del diritto alla disconnessione, necessario per tutelare i tempi di riposo e la salute del lavoratore, non può avere ripercussioni sul rapporto di lavoro o sui trattamenti retributivi."*

Anche in questo caso la legge non fornisce indicazioni su come esercitare la disconnessione, tuttavia contiene due passaggi importanti: riconduce la disconnessione medesima al diritto al riposo e alla salute; impedisce

all'impresa di comminare sanzioni o stabilire peggioramenti normativi e/o retributivi a danno dei lavoratori che esercitano il diritto alla disconnessione.

Alle leggi prima citate ha fatto seguito il recentissimo "Protocollo nazionale sul lavoro in modalità agile", siglato il 7 dicembre 2021 dal Ministro del Lavoro e numerose organizzazioni sindacali e datoriali", fra cui CGIL, CISL e UIL oltreché – per quanto interessa le nostre categorie – ABI e ANIA.

Si tratta di un testo che si apre con una premessa che è una presa di posizione veramente incondizionata e di assoluto ottimismo nei confronti del lavoro agile. Peraltro, il Protocollo non aggiunge novità di sorta rispetto alle leggi del 2017 e 2021 sul tema specifico della disconnessione; l'art. 3 si limita infatti a stabilire quanto segue:
"La prestazione di lavoro in modalità agile può essere articolata in fasce orarie, individuando, in ogni caso, in attuazione di quanto previsto dalle disposizioni normative vigenti, la fascia di disconnessione nella quale il lavoratore non eroga la prestazione lavorativa. Vanno adottate specifiche misure tecniche e/o organizzative per garantire la fascia di disconnessione."
E in concreto, le misure tecniche e/o organizzative necessarie ad assicurare la disconnessione rientrano semplicemente fra i contenuti dell'accordo individuale stipulato dal lavoratore, secondo quanto previsto dal precedente art. 2. Il che significa che sono interamente demandati alla discrezionalità del datore di lavoro.

Per avere un'idea di quali sarebbero gli interventi normativi in tema di disconnessione e a favore dei lavoratori vale la pena di leggere l'intervento dell'Avvocato Bruno Del Vecchio quale rappresentante dell'Associazione Comma 2 – che raduna diversi avvocati lavoristi "di sinistra" - tenuto il 3 novembre 2021 di fronte alla Commissione Lavoro pubblico e privato della Camera dei Deputati nel corso dell'esame di alcune proposte di legge in materia di lavoro agile.

L'Avvocato Del Vecchio osserva come tutte le proposte pongano un diritto alla disconnessione in capo al lavoratore ma non un obbligo corrispondente per il datore di lavoro. E precisa che *"Se un prestatore di lavoro ha il diritto di non rispondere (in determinati orari e in determinate situazioni), ciò non vuol dire che il datore di lavoro o chi per lui (il dirigente, ad esempio) non possa comunque inviare messaggi e richieste, anche se le stesse possono essere riscontrate in un momento successivo. Certo, il datore di lavoro può anche non avere il diritto ad una risposta immediata, ma comunque, per il prestatore di lavoro una mail, un messaggio sono sempre una pressione, professionale e psicologica (e per superare questa "pressione", la risposta immediata è sovente quella ritenuta più efficace e "liberante"). Non si può dire, quindi, che è sufficiente non rispondere, se previsto dagli accordi o dalla normativa di fonte superiore, oppure che basta non "aprire" la comunicazione. Oltre al diritto alla disconnessione, quindi, è auspicabile che si preveda uno specifico obbligo del datore di lavoro (e di chi per lui) a non connettersi con il prestatore di lavoro. Un obbligo che, se non rispettato, possa prevedere un efficace sistema sanzionatorio."*

In estrema sintesi, il diritto alla disconnessione non si realizza consentendo al lavoratore di disconnettersi – probabilmente non lo farà – ma vietando al datore di lavoro di connettersi con il lavoratore in certe fasce e stabilendo una sanzione in caso mancato rispetto del divieto: il diritto alla disconnessione in capo al lavoratore deve diventare un obbligo alla disconnessione in capo al datore di lavoro.

Passiamo ora alla risoluzione del Parlamento Europeo del 21 gennaio 2021 sul diritto alla disconnessione, assai più articolata e sfaccettata rispetto al Protocollo che dovrà disciplinare il lavoro agile in Italia. Non si tratta di un testo di legge vincolante per gli stati membri ma semplicemente di una sorta di esortazione o invito nei confronti della Commissione Europea a emanare una direttiva in materia; una bozza di tale direttiva è allegata alla

risoluzione e si pone come un'indicazione dei principi giuridici ai quali dovrebbe attenersi la futura direttiva.

La risoluzione vera e propria è preceduta da una vasta premessa che illustra i più recenti sviluppi del lavoro agile in Europa dopo l'epidemia. In primo luogo, evidenzia che tale modalità di lavoro *"consente una libertà, indipendenza e flessibilità maggiori per organizzare meglio l'orario di lavoro e le mansioni lavorative, ridurre il tempo impiegato per raggiungere il luogo di lavoro e facilitare la gestione degli obblighi personali e famigliari, creando in tal modo un equilibrio migliore tra vita privata e vita professionale"* (premessa 1).

Ma subito dopo sottolinea che *"l'essere costantemente connessi, insieme alle forti sollecitazioni sul lavoro e alla crescente aspettativa che i lavoratori siano raggiungibili in qualsiasi momento, può influire negativamente sui diritti fondamentali dei lavoratori, sull'equilibrio tra la loro vita professionale e la loro vita privata, nonché sulla loro salute fisica e mentale e sul loro benessere*" (premessa 2).

E più in generale evidenzia che il lavoro a distanza *"può avere un impatto negativo sulla qualità dell'orario di lavoro e sull'equilibrio tra vita professionale e vita personale, così come sulla salute fisica e mentale; (…) emergono difficoltà particolari quando l'attività lavorativa non è legata a un luogo specifico, quando la connettività per il lavoro è costante e quando il lavoro occupa del tempo che dovrebbe essere dedicato alla famiglia e alla vita privata"* (premessa 8).

Procedendo, la premessa 10 evidenzia un dato di fatto che fino a due anni fa era del tutto scontato, ma purtroppo è stato messo in discussione dalle prassi più discutibili emerse nel 2020 in occasione dell'epidemia: *"secondo la legislazione attuale e la giurisprudenza della Corte di giustizia dell'Unione*

europea, i lavoratori non sono tenuti a fornire ai datori di lavoro una disponibilità costante e senza interruzioni".

Infine, la premessa 17 affronta il nodo del controllo a distanza, evidenziando che le nuove tecnologie e l'intelligenza artificiale *"non dovrebbero condurre a un uso disumanizzato degli strumenti digitali né sollevare preoccupazioni relative alla vita privata e a una raccolta dei dati personali, una sorveglianza e un controllo sproporzionati e illegali dei lavoratori; (…) i nuovi strumenti di sorveglianza del luogo di lavoro e delle prestazioni lavorative, che consentono alle imprese di tracciare ampiamente le attività dei lavoratori, non dovrebbero essere visti come una possibilità per effettuare una sorveglianza sistematica dei lavoratori."*

Si tratta di considerazioni assolutamente chiare e tali da non richiedere chiarimenti particolari.

Nell'articolato vero e proprio della bozza di direttiva allegata alla risoluzione del Parlamento Europeo appaiono di particolare rilievo gli art. 2, 3 e 4.

L'art. 2 fornisce la seguente definizione della disconnessione: *"il mancato esercizio di attività o comunicazioni lavorative per mezzo di strumenti digitali, direttamente o indirettamente, al di fuori dell'orario di lavoro"*.

Ne consegue che la disconnessione avviene con "la messa a riposo" degli strumenti di lavoro digitale – e quindi è peculiare di tali strumenti – una volta terminato l'orario lavorativo: s'identifica quindi un nesso fra disconnessione e orario, concetto quest'ultimo che poco per volta è diventato sempre più sbiadito per effetto del lavoro agile.

L'art. 3 è consequenziale al concetto espresso nel precedente art. 2.

Gli Stati membri garantiscono che i datori di lavoro prendano i provvedimenti necessari per fornire ai lavoratori i mezzi per esercitare il diritto alla disconnessione.
Gli Stati membri garantiscono che i datori di lavoro istituiscano un sistema oggettivo, affidabile e accessibile che consenta la misurazione della durata dell'orario di lavoro giornaliero svolto da ciascun lavoratore, nel rispetto del diritto dei lavoratori alla vita privata e alla tutela dei dati personali. I lavoratori possono richiedere e ottenere il registro del loro orario di lavoro.

Si tratta di una disciplina che si presta a una doppia chiave di lettura. Da una parte può apparire costrittiva nei confronti del lavoratore, oltreché estranea all'impostazione del lavoro agile e alle previsioni di molti CCNL e accordi sindacali in materia. Ma d'altra parte può consentire – quanto meno - il riconoscimento degli straordinari e delle prestazioni aggiuntive nei giorni festivi e soprattutto può arginare il rischio che il lavoro agile debordi sino a rendere ogni giornata una commistione indistinta di spazi e tempi di lavoro e di vita privata, in cui i concetti di orario di lavoro e anche di giorni lavorativi e giorni festivi diventano evanescenti, soprattutto dopo le prassi più discutibili emerse nel 2020 in occasione dell'epidemia.

L'art. 4 pone a carico degli stati membri la disciplina delle modalità per attuare la disconnessione, precisando che tali modalità siano stabilite previa consultazione con le parti sociali. Le normative statali dovranno stabilire fra l'altro:

- le modalità pratiche per scollegarsi dagli strumenti digitali;
- il sistema per la misurazione dell'orario di lavoro;
- valutazioni della salute e della sicurezza, comprese le valutazioni del rischio psicosociale, in relazione al diritto alla disconnessione;
- le possibili deroghe al diritto alla disconnessione, deroghe possibili soltanto in circostanze eccezionali e motivate - quali la forza maggiore o altre emergenze – e a fronte di una compensazione retributiva.

È da segnalare che fra le parti sociali che saranno consultate nell'iter legislativo possono essere sicuramente presenti i sindacati dei lavoratori. Inoltre, si prevede che la legislazione stabilisca per la disconnessione modalità dettagliate: per fare un esempio, le previsioni della legge italiana n. 81/2017 non appaiono adeguate a tale indicazione. Sono possibili delle deroghe ma assai circoscritte e compensate da una voce retributiva: è il caso già noto della reperibilità prevista dai contratti collettivi per certe categorie di lavoratori, ai quali spetta una specifica indennità. Infine, è di tutto rilievo la previsione che la valutazione del rischio debba essere estesa agli aspetti psicosociali, che sono emersi in modo netto dal 2020.

La direttiva proposta con la risoluzione del 21 gennaio 2021 stabilisce due possibilità agli stati nazionali: la prima è quella di emanare leggi coerenti con i requisiti minimi della direttiva stessa, tali leggi possono essere integrate da accordi collettivi; la seconda è quella di delegare la normativa agli accordi collettivi che dovranno comunque rispettare i requisiti minimi. Come di consueto, tale seconda ipotesi potrebbe presentare il rischio derivante dai rapporti di forza ben diversi fra imprese e sindacati, specie in certi settori produttivi.

PRIVACY E VIRTUALITA'

1. Come e quando nasce il diritto alla privacy

Quando si parla di virtualità e nel nostro caso specifico di smart working, si parla di innovazione, di progresso, di welfare, ma il rischio più grande che si corre è pensare che debbano essere creati nuovi diritti in aggiunta ai diritti preesistenti, sottovalutando la tutela di questi ultimi, in particolar modo per quanto riguarda il collegamento con la privacy, che andrebbe invece ancor più rafforzato.

Per non correre il rischio che lasciando il vecchio per il nuovo ci si dimentichi che senza il rispetto dei diritti fondamentali non solo non godremmo dei vantaggi della virtualità ma rischieremmo un peggioramento delle condizioni lavorative, dedichiamo l'attenzione a rispolverare l'origine e le basi dei diritti connessi al rapporto tra lo smart working e la privacy.

Facciamo fondamentalmente un passo indietro per poter andare avanti raccontando come e quando è nato il diritto alla privacy.
Ci troviamo alla fine dell'800 a Boston, città ricca e fiorente che ospita la sede universitaria di Harvard e caratterizzata da un'intensa vita mondana. Di questa vita mondana si occupano molti giornali, che ne riportano i dettagli più interessanti. Una delle protagoniste di queste cronache è la signora Warren, moglie di un giovane avvocato di Boston, che inizia a comparire spesso sulle colonne della "evening gazzette".
La signora, come riportavano i giornali, tornava tardi la sera spesso accompagnata da gentiluomini che non erano il marito, e l'avvocato Warren non apprezzando tali cronache, e considerando che la "evening gazzette" marciava a un ritmo di 80000 copie al giorno, decise di fare causa al giornale.

L'avvocato Warren, pur nel rispetto della libertà di espressione tanto cara agli Stati Uniti, ritenne infatti che il limite fosse stato ampiamente superato e quindi fa causa al giornale insieme a un suo giovane collega di studio, Louise Braundis, che diventerà giudice della Corte suprema americana.
Sia Warren sia Braundis non erano solo dei brillanti avvocati ma anche dei raffinati giuristi che decisero di scrivere un saggio sulla causa, pubblicato nel 1890 sulle pagine della "Harvard law review" che si intitola "the right to privacy" e segna l'atto di nascita del diritto alla privacy.
Nel saggio i due giuristi definiscono la privacy con l'espressione " the right to be left alone", ovvero il diritto di essere lasciati soli per godere in pace della propria vita. È la stessa logica che troviamo nel diritto di proprietà

privata, ovvero nel diritto di non subire intromissioni nella propria abitazione.
È evidente qui la matrice liberale di questo diritto, con questa idea di libertà in senso negativo, come non interferenza nella sfera dell'individuo, a meno che, ci indicano Warren e Braundis, non si rivesta un ruolo pubblico, e in questo caso deve prevalere la libertà di cronaca, perché c'è un interesse pubblico di mezzo.
Per esempio un uomo politico non può invocare il diritto alla privacy per sottrarsi al controllo democratico sulle sue azioni. Questo inquadramento è tutt'ora attuale, il diritto alla riservatezza da un lato e la libertà di cronaca e di espressione dall'altro, rappresentano ancora oggi i punti cardini su cui si basa la disciplina della privacy con i dovuti bilanciamenti tra gli opposti interessi in gioco.

Ma lasciamo gli Stati Uniti per andare in Europa, dove dagli anni '60 si comincia concretamente a parlare di diritto alla privacy fino alla sua consacrazione nella carta dei diritti fondamentali dell'Unione Europea del 2000, che inserisce la privacy tra i diritti dei cittadini europei e poi più recentemente con il General data protection regulation, il Gdpr, cioè il regolamento generale sulla protezione dei dati personali del 2016.

Prima di parlare del Gdpr restano altre due cose importanti da dire sulla privacy: l'esordio del diritto alla privacy era quindi il diritto ad essere lasciati soli, ma nel corso del tempo si arricchisce di una serie di significati ulteriori che possiamo identificare in due nuclei fondamentali: il primo è quello che corrisponde al nucleo originario, ovvero alla tutela della riservatezza della nostra vita privata, che troviamo nell'art. 7 della Carta dei diritti fondamentali dell'Unione Europea.
La giurisprudenza italiana comincia ad occuparsene nel 1950, il primo caso ad arrivare in Cassazione nel 1956 riguarda il grande tenore Enrico Caruso. Pochi anni prima era uscito nelle sale un film chiamato "Enrico Caruso, leggenda di una voce", con una giovanissima Gina Lollobrigida che

raccontava la vita del tenore. Caruso era popolarissimo tra la gente e il film aveva avuto molto successo, ma non era per nulla piaciuto agli eredi di Enrico Caruso, secondo loro il film gettava in pasto alla curiosità del pubblico alcuni aspetti intimi e riservati della vita del tenore, e così avevano fatto causa alla casa produttrice del film.
La Cassazione però non accoglie la richiesta di risarcimento danni, cosa che invece farà qualche anno dopo quando condannerà la rivista "il tempo" a risarcire gli eredi di Claretta Petacci, la storica amante di Benito Mussolini, per una serie di articoli lesivi della sua riservatezza in assenza di un interesse pubblico. Ma c'è dell'altro perché col tempo i giudici hanno cominciato a leggere quel riferimento alla riservatezza della vita privata in senso più ampio, come diritto a fare le nostre scelte di vita al riparo dal controllo pubblico e dalla stigmatizzazione sociale. Ne è un esempio la legalizzazione dell'aborto, realizzatasi sulla base di quanto contenuto nel diritto alla privacy, inteso come diritto alla libera scelta della donna per ciò che attiene alle scelte più intime e private della vita. È interessante il percorso interpretativo che ne fanno i giudici, prendono quel diritto ad essere lasciati soli, a non subire interferenze nella propria vita privata e lo applicano all'ambito delle scelte di vita individuali.

Chiarita l'origine della privacy, andiamo alla parte che ci interessa che è la tutela dei dati personali, citandone le fonti per potere avere gli strumenti per un corretto bilanciamento tra gli interessi opposti in gioco, che nel nostro caso vedranno come protagonisti la riservatezza del lavoratore e la possibilità del datore di lavoro di invaderne i confini, nel rispetto delle normative.

Il secondo nucleo dei diritti alla privacy è la protezione dei dati personali tutelata dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea, nonché terreno di gioco del nostro Gdpr. Mentre prima parlavamo di non interferenza, qui ci muoviamo su un altro livello perché si tratta di stabilire come gestire questi dati, come conservarli, per quali scopi

trattarli e tanto altro ancora. E qui veniamo a un punto importante: la tutela dei nostri dati personali è uno strumento per proteggere la nostra vita privata da indebite interferenze e quindi esiste senz'altro un collegamento tra il primo e il secondo nucleo della privacy e quindi perfettamente possibile che si ponga una questione di tutela dei dati personali a prescindere da una violazione della nostra vita privata e familiare. Quindi la privacy e la protezione dei dati personali, per quanto siano due cose collegate tra di loro non sono dei sinonimi, anche se spesso la prassi sembra suggerirlo.

Molto spesso infatti ci sono persone che parlano genericamente di privacy quando in realtà intendono specificamente riferirsi alla protezione dei dati personali, al punto che lo stesso Garante per la protezione dei dati personali si è dovuto adeguare.

Il Garante, lo ricordiamo, è un'autorità amministrativa indipendente istituita nel 1996 e che si occupa, come suggerisce la denominazione, della tutela dei nostri dati personali. Se però andate a vedere il sito del Garante scoprirete che come nome di dominio troverete Garante della privacy.it, proprio per farsi trovare più facilmente nei risultati dei motori di ricerca.

La necessità di creare delle figure di supporto alla tutela dei dati personali nasce dall'aumento del valore del bene protetto.

2. Il Gdpr e il trattamento dei dati personali

Si dice infatti spesso che il petrolio del XXI secolo non si trova nel sottosuolo ma nel web sotto forma di dati, chi è in grado di estrarre informazioni dai dati come il petrolio dal sottosuolo ha in mano le chiavi del mondo in cui viviamo. Opportunamente incrociati e aggregati i dati sono in grado di fornirci una miriade di informazioni con enormi ricadute per la ricerca, lo sviluppo, il business, le strategie politiche. Pensate per esempio alle politiche sanitarie, in tempo di pandemia, conoscere i dati di sviluppo del contagio, i dati di accesso agli ospedali, la gestione dei posti in rianimazione, lo spostamento delle persone, sono tutte informazioni

essenziali per gestire efficacemente un'emergenza sanitaria. Ed è in questo quadro che si inserisce il regolamento generale per la protezione dei dati, il Gdpr, che detta regole comuni a tutti i 27 paesi membri dell'Unione Europea. Più precisamente il Gdpr si occupa della tutela dei dati personali delle persone fisiche.

Partiamo dal concetto di persone fisiche: le persone fisiche non sono altro che le persone in carne ed ossa, dunque il Gdpr si applica solo ai dati personali delle persone fisiche e non si applica ai dati delle imprese, delle pubbliche amministrazioni, delle associazioni, in generale a tutte quelle che il diritto chiama persone giuridiche. In questo senso potremmo dire che il Gdpr ha un'impostazione antropocentrica.

Vediamo ora che cosa sono i dati personali: sono dati personali tutte le informazioni che consentono di identificare una persona fisica in modo diretto (per esempio nome, cognome, o una fotografia del viso) oppure indiretto (per esempio il numero di targa o il codice fiscale) e che forniscono informazioni sulle sue caratteristiche fisiche, il suo stile di vita, le sue relazioni, il suo stato di salute, la sua situazione economica e sociale, la sua religione o l'adesione ad un partito politico. Da questa definizione deduciamo quindi che i dati personali si possono presentare in forme molto diverse e siamo in grado di definire per esclusione quali dati non sono dati personali, e quindi non sono soggetti a Gdpr. Non sono dati personali i dati anonimi e i dati anonimizzati, cioè resi anonimi in un secondo momento.

Entrambi escludono che si possa risalire all'identità della persona interessata e perciò il Gdpr non si applica. Un esempio di dati anonimi può essere quello dei dati statistici, che sono o anonimi in partenza o anonimizzati in un secondo momento.

I dati personali si dividono in due gruppi, il primo gruppo è quello dei dati comuni, così chiamati perché non rivelano aspetti particolarmente intimi della nostra vita. Ne fanno parte, per esempio, i dati anagrafici, il codice fiscale, il numero di targa, la residenza e l'indirizzo IP.

Nel secondo gruppo invece troviamo i più personali dei dati personali che il Gdpr chiama "categorie particolari di dati personali". Prima del Gdpr venivano chiamati "dati sensibili" proprio perché rivelano aspetti intimi e personali della nostra vita. Appartengono alle categorie particolari di dati personali: la nostra origine razziale o etnica, il nostro stato di salute, la nostra vita sessuale o orientamento sessuale, le nostre opinioni politiche, l'appartenenza ad un sindacato, la nostra confessione religiosa e i nostri eventuali trascorsi giudiziari. Ancora rientrano tra i dati particolari i dati genetici, come il DNA e i dati biometrici, che identificano in modo univoco la nostra persona. Può darsi che quest'ultima categoria suoni poco familiare ma chissà quanti sbloccano lo smartphone utilizzando l'impronta digitale o il riconoscimento facciale: questi sono dati biometrici, così come lo sono la forma dell'iride, la nostra immagine scansionata all'aeroporto per il controllo passeggeri, la tonalità della nostra voce e così via.

Perché è importante distinguere i dati comuni dalle categorie particolari di dati personali? È importante perché per le categorie particolari di dati personali, e solo per quelle, il Gdpr pone come regola generale quella del divieto di utilizzo. La regola è che non si possono usare, l'uso è da considerarsi del tutto eccezionale e deve ubbidire a standard di sicurezza più elevati. Per esempio, la richiesta di un consenso esplicito dell'interessato nell'uso di quelle specifiche categorie di dati.

Ora che sappiamo che cosa sono i dati personali dobbiamo chiederci in che modo devono essere maneggiati, gestiti, conservati, in una parola: trattati. Partiamo proprio dalla definizione di trattamento dei dati personali che ci è fornita dal Gdpr: costituisce un trattamento qualsiasi operazione applicata ai dati personali compiuta con senza l'aiuto di processi automatizzati. Raccogliere dati, conservarli in archivio, sono tutti esempi di trattamento. Se per esempio sono un ecommerce e conservo gli indirizzi email degli iscritti alla mia newsletter sto facendo un trattamento, se sono un medico e sto archiviando i dati sanitari dei miei pazienti, sto facendo un trattamento.

Quindi vediamo quali regole detta il Gdpr per il trattamento dei dati personali analizzando un caso pratico.

3. Caso pratico: Garante per la protezione dei dati personali, ordinanza ingiunzione nei confronti di Comune di Bolzano del 13/05/2021 n. 190.

LA NAVIGAZIONE IN INTERNET DEI DIPENDENTI

L'ordinanza ingiunzione nei confronti del Comune di Bolzano del 13/05/2021 del Garante per la protezione dei dati personali riguarda la navigazione in Internet dei dipendenti ed è strettamente correlata al rispetto del principio di liceità, correttezza e trasparenza del trattamento dei dati relativi alla navigazione.
L'informativa agli interessati è fondamentale perché il trattamento dei dati si svolga nel rispetto dei principi suddetti.

Nel caso di specie, con un reclamo, una dipendente del Comune di Bolzano ha lamentato delle presunte violazioni della disciplina di protezione di dati personali con riguardo al trattamento di dati posti in essere dall'Ente mediante il monitoraggio del traffico di rete e dei singoli accessi ad Internet effettuati dall'interessato e, in generale, dai dipendenti comunali.

Il dipendente ha lamentato che l'Ente avrebbe trattato dati personali relativi alla sua navigazione in Internet, durante l'orario di lavoro, e, di aver ricevuto una comunicazione di avvio procedimento disciplinare, dove gli veniva contestato che era stato collegato in un periodo specifico con il computer del Comune, per oltre 40 minuti a facebook, e per più di 3 ore a youtube, per consultare pagine Internet non inerenti il suo lavoro come risultanti dai tabulati del traffico dati del Comune di Bolzano. Questi dati poi sono stati usati per iniziare il procedimento disciplinare che è stato poi

successivamente archiviato per ragioni inerenti all'inattendibilità dei dati raccolti.

Riportiamo gli stralci dell'ordinanza più salienti: "il Comune ha adottato, fin dal 2000 (cfr. accordo sindacale del 20.10.2000 per l'utilizzo dei servizi di rete, integrato il 25.3.2010, limitatamente ad alcuni aspetti), un sistema che consente il tracciamento generalizzato (ed ex ante) degli accessi ad Internet da
parte dei dipendenti e la memorizzazione, per trenta giorni, di informazioni di natura personale ("giorno, ora, nome utente, PC utilizzato e sito consultato").

Il trattamento risulta essere stato effettuato in violazione dell'obbligo previsto dall'art. 13 del Regolamento, nonché - attesa la frammentarietà delle informazioni contenute in molteplici atti, diversi per natura e funzione, stratificatisi nel tempo dall'amministrazione - non in conformità al
principio di correttezza e trasparenza e dunque in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento.

In base al Regolamento, il trattamento deve essere "necessario" rispetto alla lecita finalità perseguita (art. 6, par. 1 del Regolamento) e avere ad oggetto i soli dati "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c), del Regolamento).

In tale contesto, l'amministrazione ha stipulato un accordo con le organizzazioni sindacali - dapprima nel 2000, poi aggiornato nel 2010 e, da ultimo, in data XX 2020 (cfr. all. n. 11, alla nota del XX, in atti) - come prescritto dalla disciplina in materia di impiego di sistemi tecnologici sul
posto di lavoro (art. 4 della legge n. 300 del 1970) che, anche a seguito delle modifiche disposte dal decreto legislativo 14 settembre 2015, n. 151,

consente l'impiego di "impianti audiovisivi e [di] altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori [...] esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale", nel rispetto di specifiche condizioni, quali il previo accordo con la rappresentanza sindacale unitaria o le rappresentanze sindacali aziendali, ovvero, in alternativa, previa autorizzazione delle sedi territoriali dell'Ispettorato nazionale del lavoro (comma 1). Peraltro anche il Garante, dopo le modifiche apportate nel 2015 a tale quadro di settore, si è espresso, proprio in merito all'utilizzo di sistemi che comportano la tracciatura degli accessi a Internet (cfr. provvedimento del 13 luglio 2016, n. 303, doc. web n. 5408460, confermato dal Tribunale di Chieti con sentenza n. 672 del 24 ottobre 2019) precisando, tra l'altro, che tali sistemi richiedono le garanzie di cui all'art. 4, comma 1 della l. 300 del 1970, non potendo essere ricompresi nel novero degli "strumenti di lavoro", ai sensi dell'art. 4, comma 2, diversamente dai sistemi di inibizione automatica di consultazione di contenuti in rete.

Nel rispetto del principio di "liceità, correttezza e trasparenza", il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12 del Regolamento).

Nel premettere che, solo dal 2015, il quadro normativo vigente consente che i dati raccolti ai sensi dell'art. 4, commi 1 e 2 della legge n. 300/1970 possano essere utilizzati dal datore di lavoro "a tutti i fini connessi al rapporto di lavoro" a condizione che "sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n.196" (art. 4, comma 3 l. n. 300/1970), si osserva quanto segue.

Nel caso di specie risulta, invece, che i dati relativi alla navigazione web del reclamante, originariamente raccolti e trattati tramite il citato sistema in modo non proporzionato e non conforme alla disciplina in materia di protezione dei dati personali, in violazione dell'art. 5, par. 1, lett. a) e c), 6 del Regolamento e dell'art. 113 del Codice, e senza un'adeguata informativa ai sensi dell'art. 13 del Regolamento, siano stati successivamente impiegati per contestare addebiti disciplinari allo stesso, non rispettando quindi i presupposti e le condizioni previste dalla richiamata disciplina di settore all'art. 4, comma 3, della legge n. 300 del 1970."

Il Garante ha in definitiva rilevato l'illiceità del trattamento effettuato dal Comune di Bolzano per violazione degli artt. 5, 6, 9, 88 e 35 del Regolamento, nonché 113 e 114 del Codice nei termini di cui in motivazione e dichiara ai sensi dell'art. 2-decies del Codice l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali.