



Numero 4 / 2021

Antonio Ciccia Messina e Ivan Libero Nocera

***Privacy* e processo del lavoro: il requisito
della conformità alla disciplina sulla tutela
della riservatezza**

***Privacy* e processo del lavoro: il requisito della conformità alla disciplina sulla tutela della riservatezza**

Antonio Ciccia Messina e Ivan Libero Nocera

Abstract

Nel corso del processo del lavoro il Giudice è chiamato a valutare il rispetto della disciplina della privacy ad opera del datore di lavoro a riguardo dell'utilizzo ai fini disciplinari delle informazioni raccolte con impianti e strumenti usati in azienda.

Pertanto, la subordinazione dell'utilizzo processuale di tali informazioni al rispetto della disciplina sulla privacy non può riguardare quelle disposizioni della disciplina sulla privacy non rilevanti rispetto al rapporto sostanziale (intercorrente tra lavoratori e datori di lavoro), quali ad esempio adempimenti organizzativi a carico del titolare del trattamento.

Rientrano, invece, tra le disposizioni rilevanti le disposizioni sulle informative e sulla base giuridica così come sui principi e sui diritti spettanti al lavoratore in quanto interessato.

===

During the job's trials, the Judge is called upon to assess the employer's compliance with the privacy regulations regarding the use for disciplinary purposes of the information gathered with companies' systems and tools. Moreover, the subordination of the use as evidence of such information to compliance with the privacy regulations cannot concern those provisions of the privacy regulations that are not relevant to the employment relationship, such as organizational obligations borne by the data controller.

On the contrary, the relevant provisions that have to be considered are the provisions on information and on the legal basis as well as on the principles and rights of the worker as a data subject.

1. PREMESSA

Com'è noto, l'art. 88 GDPR autorizza gli Stati a prevedere, tramite accordi collettivi o disposizioni legislative, regole particolari volte ad assicurare la protezione dei diritti e delle libertà dei dipendenti durante i trattamenti dei dati nel contesto del rapporto di lavoro. Ciò in quanto le attività di controllo del lavoratore devono svolgersi in un contesto di trasparenza e di adeguata protezione dei dati personali, in ciascuna delle molteplici fasi del rapporto di lavoro: valutazione candidati e assunzione, valutazione delle prestazioni lavorative, pianificazione ed organizzazione della prestazione lavorativa, salute e sicurezza dell'ambiente di lavoro, protezione dei beni del dipendente, conclusione del rapporto di lavoro.

Pertanto, l'art. 88 GDPR individua un particolare spazio regolativo che, implementi la materia attraverso la predisposizione di misure adeguate a tutelare «la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro».

Tuttavia, il grado di esaustività precettiva delle disposizioni in materia di rapporto tra disciplina della *Privacy* e regole di giudizio per il processo del lavoro è tanto basso da poter essere ritenuto inesistente.

Ciò porta alla inevitabile conseguenza dell'amplificazione della possibile aleatorietà delle decisioni sull'ammissibilità delle fonti di prova e, a cascata, dell'esito sostanziale della lite.

Si tratta, peraltro, di una aleatorietà che non rientra nella sfera fisiologica di assunzione del rischio processuale addossabile alle parti, ma di una

aleatorietà sproporzionata, eccessiva ed intollerabile, dovuta alla incapacità del legislatore di redazione di un testo normativo idoneo a:

- a) descrivere una regola, una qualsiasi;
- b) prescrivere con esattezza la tenuta delle condotte obbligatorie e l'omissione delle condotte vietate;
- c) servire da parametro del controllo nomofilattico delle decisioni assunte dai Giudici.

In questa breve nota, dunque, ci si propone di analizzare lo stato della legislazione vigente e, in particolare, da un lato, l'art. 4, comma 3, St. Lav. e, dall'altro lato, gli articoli 2-*decies* e 160-*bis* Cod. *Privacy* (D.lgs. 196/2003). Quindi l'indagine descriverà le lacune di esaustività e concludenza delle disposizioni (tanto macroscopiche da poter essere percepite anche a una lettura rapida) per poi tentare di proporre possibili soluzioni di ripiego, nell'attesa di un ravvedimento operoso del legislatore.

2. LO STATO DELLA LEGISLAZIONE VIGENTE

L'art. 2-*decies* del Codice della *Privacy* prevede l'inutilizzabilità dei dati e così si esprime:

“I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'articolo 160-bis.”.

L'art. 160-*bis* del codice della *Privacy* costituisce una eccezione alla riportata regola dell'inutilizzabilità per violazione della *Privacy*.

Tale eccezione si applica al “procedimento giudiziario” e, in tale contesto, *“la validità, l'efficacia e l'utilizzabilità ... di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento (Ue n. 2016/679, alias Gdpr, ndr) restano disciplinate dalle pertinenti disposizioni processuali”.*

Stando alle disposizioni sopra riportate, le regole processuali sulle prove e, quindi, le conseguenti regole di giudizio non sono in nulla interessate dalle disposizioni rilevanti in materia di *Privacy*.

Altrimenti detto, in generale, nel processo, le regole tratte dalla normativa settoriale sulla *Privacy*, a riguardo della conformità dei trattamenti, sono da considerarsi *tamquam non essent*.

In questo quadro bisogna, a questo punto, inserire l'art. 4 dello Statuto dei Lavoratori (legge 300/1970), nel cui comma 3 si legge: “*Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili 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.*”.

Quest'ultima disposizione si riferisce alle informazioni raccolte da strumenti di controllo indiretti (St. Lav., art. 4, comma 1) e da strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa oltre che da strumenti di registrazione degli accessi e delle presenze.

In questo ambito di applicazione (pur ambiguamente descritto), la disposizione detta due condizioni ai fini della legittimità dell'utilizzo delle informazioni raccolte comunque connesse al rapporto di lavoro, inclusi, quindi, le informazioni inerenti all'applicazione di sanzioni disciplinari.

La prima condizione consiste in un obbligo di trasparenza, dal duplice oggetto.

Il primo oggetto degli obblighi di trasparenza onera il datore di lavoro (se vuole utilizzare le informazioni raccolte) a dare notizie su come funzionano gli strumenti utilizzati (sia gli strumenti di controllo indiretto sia gli strumenti di lavoro sia gli strumenti di registrazione accessi e presenze).

La trasparenza, appena citata, è da considerare, per usare un'immagine, alla stregua di un foglio di istruzioni tecniche su come funzionano gli apparecchi utilizzati.

Il secondo oggetto degli obblighi di trasparenza onera il datore di lavoro (sempre se vuole utilizzare le informazioni raccolte) a dare notizie su come effettuerà i “controlli”.

Non è il cuore del problema affrontato in questo breve saggio, ma è disdicevole che il legislatore usi in maniera così sciatta la parola “controlli”, senza chiarire di quali controlli stia parlando.

La scrittura poteva essere decisamente più chiara. Peraltro, il senso dovrebbe essere il seguente: il datore di lavoro effettua controlli relativi all’organizzazione e alla produzione, alla sicurezza del lavoro e alla tutela del patrimonio aziendale; nel corso di questi controlli, gli strumenti utilizzati non possono non raccogliere informazioni sui lavoratori.

Da tutto ciò deriva che il secondo oggetto degli obblighi di trasparenza onera il datore di lavoro (se vuole utilizzare le informazioni raccolte) a dare notizie su come funzionano gli strumenti utilizzati per i controlli relativi all’organizzazione e alla produzione, alla sicurezza del lavoro e alla tutela del patrimonio aziendale; tali notizie devono chiarire quali sono le informazioni sui lavoratori che gli strumenti utilizzati non possono non raccogliere.

Va sottolineato, fin da subito, che la disposizione, di cui stiamo parlando (informazione sulle modalità dei controlli), non riguarda i controlli effettuati “per controllare direttamente i lavoratori” (da considerarsi vietati, nonostante l’abbandono della chiara formulazione originaria del comma 1 dell’art. 4 dello St. Lav.) e non riguarda, neppure, gli strumenti utilizzati per scovare l’autore di illeciti già subiti dal datore di lavoro.

A proposito di tale ultima finalità, si sottolinea che si tratta, infatti, di controlli per l’esercizio del diritto di difesa in concreto o, se si vuole, “*ex post*” rispetto a un attacco alla sfera patrimoniale dell’imprenditore: siamo, quindi, nell’ambito di una finalità del tutto diversa dalle finalità citate dal primo comma dell’art. 4 dello St. Lav., tra cui la pianificazione della tutela del patrimonio aziendale predisposta *ex ante* rispetto alla commissione di attacchi.

La seconda condizione della legittimità dell'utilizzo delle informazioni raccolte a tutti i fini connessi al rapporto di lavoro è il rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196 (Codice della *privacy*).

A tale proposito si rimarca che, per effetto dell'art. 1 del Codice della *Privacy*, la seconda condizione, di cui si sta parlando, è da riferire anche alle norme del regolamento (UE) 2016/679.

Pertanto, la legittimità dell'utilizzo delle informazioni raccolte (con strumenti di controllo indiretto, strumenti di lavoro e di registrazione di accessi e presenze) a tutti i fini connessi al rapporto di lavoro dipende dal rispetto sia del codice della *Privacy* sia del Regolamento Ue 2016/679.

Pertanto, sintetizzando, abbiamo:

- a) la regola: inutilizzabilità dei dati trattati in violazione della disciplina normativa della *Privacy*;
- b) l'eccezione alla regola: utilizzabilità nel processo dei dati dei dati trattati in violazione della disciplina normativa della *Privacy*, previo filtro giudiziale in applicazione delle leggi processuali;
- c) l'eccezione alla eccezione: inutilizzabilità, ai fini connessi al rapporto di lavoro, delle informazioni raccolte in violazione della disciplina normativa della *Privacy*, con strumenti di controllo indiretto, strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e di registrazione accessi e presenze.

3. LE LACUNE DI ESAUSTIVITÀ E CONCLUDENZA

Su tale ultima sfaccettatura (inutilizzabilità processuale dei dati raccolti in violazione delle disposizioni delle *Privacy*) poggia la constatazione di quanto l'art. 4, comma 3, St. Lav. sia carente di esaustività e concludenza. A ben vedere, il richiamo dell'intero *corpus* del Codice della *Privacy* implica anche l'applicazione dell'art. 160-*bis* con effetto auto-abrogante del più volte citato comma terzo dell'art. 4 dello Statuto dei lavoratori.

Non ritenendo plausibile che il legislatore abbia scritto una disposizione suicida, si deve passare a una lettura del richiamo al Codice della *Privacy*, escluso l'art. 160-*bis*, anch'esso più volte richiamato.

Peraltro questa correzione interpretativa è solo la prima precauzione che l'operatore deve osservare, in quanto residuano altri macigni ermeneutici. Si consideri, infatti, che, escluso l'art. 160-*bis* del Codice della *Privacy*, da un punto di vista della formulazione letterale, tutte le altre previsioni, una per una, del Gdpr e del Codice della *Privacy* devono essere esattamente adempiute a pena, per il datore di lavoro, di non poter utilizzare, ai fini connessi con il rapporto di lavoro, le informazioni raccolte con gli strumenti di controllo indiretto, con gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e con gli strumenti di registrazione degli accessi e delle presenze.

Si tratta di un *mare magnum* di prescrizioni, caratterizzate da una amplissima eterogeneità di struttura e di *ratio*, di valore cogente o monitorio, alcune sostanziali e relative al rapporto con gli interessati, altre formali e relative all'organizzazione interna o alla sicurezza informatica.

Già solo per tale motivo, si comprenderà lo stupore dell'interprete che voglia dare un orientamento pratico al datore di lavoro, considerato che ci si deve interrogare se l'utilizzo a fini disciplinari delle informazioni raccolte a carico di un dipendente sia subordinato, ad esempio, al rispetto dell'obbligo di tenere aggiornato il registro del trattamento (art. 30 Gdpr). L'ampiezza della formulazione normativa (ovvero dell'art. 4, comma 3, nella parte in cui pretende il rispetto di tutta la disciplina *Privacy*) rende imprevedibile quale inosservanza del Gdpr e del Codice della *Privacy* possa neutralizzare l'utilizzo probatorio di un dato raccolto nell'ambito del rapporto di lavoro; tale imprevedibilità è intollerabile da un punto di vista della politica legislativa; tale imprevedibilità può anche spingere a condotte di rinuncia del diritto o di abuso del diritto (ciò che conduce *de plano* all'ineffettività della norma).

Secondo una commendevole diversa opzione redazionale, il legislatore avrebbe potuto e dovuto precisare, enumerandole in maniera specifica e

tassativa, quali disposizioni della disciplina della *Privacy* siano così importanti da comportare, se violate, l'inibizione dell'uso processuale dei dati.

In altre parole, il legislatore, avrebbe dovuto chiarire espressamente le condizioni di deroga parziale alla disciplina riportata all'art. 160-*bis* del Codice della *Privacy* da applicarsi nei rapporti di lavoro.

La latitudine della formulazione (che coinvolge tutte, nessuna esclusa, le disposizioni della *Privacy*) è una vera e propria lacuna di esaustività e concludenza normativa, la quale, allo stato, comporta la delega alla prassi della definizione delle regole "effettive".

A tale riguardo, va detto subito che la giurisprudenza è senz'altro consapevole del fatto che l'utilizzabilità del dato porta determinanti conseguenze sulla decisione finale: l'inutilizzabilità del dato, unita all'assenza di altre fonti probatorie autonome che consentano di apprenderne la conoscenza, comporta che il fatto contestato debba ritenersi inesistente (così il Tribunale Padova sez. lav., ud. 19/01/2018, dep. 22/01/2018).

La giurisprudenza, andando al merito della questione, ha avuto occasione di valorizzare nell'argomentazione decisoria alcuni profili attinenti la disciplina della *Privacy*.

Si considerino le seguenti decisioni:

- la "chat" aziendale, destinata alle comunicazioni di servizio dei dipendenti, è qualificabile come strumento di lavoro ai sensi dell'art. 4, comma 2, St. Lav., essendo funzionale alla prestazione lavorativa, con la conseguenza che le informazioni tratte dalla "chat" stessa, a seguito dei controlli effettuati dal datore di lavoro, sono inutilizzabili in mancanza di adeguata informazione preventiva *ex* art. 4, comma 3, St. Lav. (https://www.lavorodirittieuropa.it/images/Cassazione_civile_sez._lav._22_09_2021_n._25731.pdf);
- i controlli eseguiti dal datore di lavoro contrastano con il comma 3 dell'art. 4 L. 300/1970, qualora il lavoratore non sia stato adeguatamente informato né sulla concreta possibilità, né tanto meno sulle modalità

relative a eventuali controlli da parte del datore di lavoro sul proprio computer e sulla propria e-mail aziendale (https://www.lavorodirittieuropa.it/images/Tribunale_Vicenza_28_10_2019_n.356.docx);

– viola la normativa sulla *Privacy* il datore di lavoro che controlla il dipendente disponendone il pedinamento e l'accesso all'account di posta elettronica senza dare atto delle ragioni e delle effettive modalità del controllo. Non può essere configurato come legittimo ai sensi dell'art. 4, comma 2 St. Lav. il controllo effettuato sull'account e-mail del dipendente in assenza dell'adeguata informazione prevista dall' art. 4, comma 3 St. Lav. Le predette violazioni comportano l'inammissibilità delle risultanze ottenute dai controlli occulti e, dunque, l'inutilizzabilità delle informazioni acquisite (https://www.lavorodirittieuropa.it/images/Tribunale_Milano_13_05_2019_n.17778.doc);

– i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento. Il legislatore al comma 3, nel prevedere a carico del datore di lavoro l'obbligo di fornire al suo dipendente “adeguata informazione” sulle modalità d'uso degli strumenti tecnologici e sulle modalità di effettuazione dei controlli attraverso tali strumenti, introduce implicitamente il divieto di controlli occulti sulla prestazione lavorativa. L'informativa, tuttavia, non deve ridursi ad un adempimento formale rivolto alla generalità dei lavoratori, ma deve essere esaustiva e adeguata e tale non può essere considerata l'indicazione di istruzioni relative all'uso dello strumento tecnologico, non accompagnate dalla specifica individuazione delle modalità di utilizzo che comportano l'acquisizione dei dati (https://www.lavorodirittieuropa.it/images/Tribunale_Torino_sez._lav._19_09_2018_n.1664.doc);

– la qualificazione dei dispositivi aziendali in termini di strumenti “di controllo” o “di lavoro” non può prescindere dalla scomposizione dello strumento in tutte le sue componenti hardware e software, rispetto ad ognuna delle quali dovrà essere indagata la potenzialità di controllo. Di conseguenza, anche l’informativa predisposta ai sensi del comma 3 dell’art. 4 St. lav. dovrà essere dettagliata, specifica e rivolta ai dipendenti non in modo generico, ma in base al loro utilizzo (https://www.lavorodirittieuropa.it/images/Tribunale_Torino_sez._lav._19_09_2018_n._1664.doc);

– è consentito il controllo a distanza del lavoratore tramite la posta elettronica aziendale se il datore di lavoro ne ha dato adeguato avviso. Contemperando l’interesse al controllo e la protezione della dignità e riservatezza dei lavoratori, il lavoratore può 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 (co.3); d) il controllo deve essere esperito in conformità al Codice della *Privacy*. Le regole sub a) e b), che dettano il regime autorizzatorio, non valgono per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, quali il software PRS e la email 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. Ne consegue che sia la posta elettronica che il software PRS rientrano in tale categoria, trattandosi di strumenti che, pur non avendo finalità di controllo (ma finalità lavorative) consentono il controllo “a distanza” dell’operato del lavoratore.

[https://www.lavorodirittieuropa.it/images/Tribunale sez. lav. - Roma 13 06 2018.doc](https://www.lavorodirittieuropa.it/images/Tribunale_sez._lav._Roma_13_06_2018.doc));

– ai sensi del comma 3 dell'art. 4 St. lav. la utilizzabilità dei dati raccolti attraverso gli strumenti di controllo a distanza ovvero attraverso gli strumenti di cui al comma 2 per tutte le finalità connesse al rapporto di lavoro è subordinata alla condizione che sia data al lavoratore adeguata informazione delle modalità di uso degli strumenti e di effettuazione dei controlli. Non può essere considerata idonea a tali fini la dicitura, generica e tautologica, contenuta nel contratto di lavoro di essere a conoscenza delle norme disciplinari relative al rapporto ([https://www.lavorodirittieuropa.it/images/Tribunale Pescara 25 10 2017.doc](https://www.lavorodirittieuropa.it/images/Tribunale_Pescara_25_10_2017.doc));

– non sono utilizzabili a fini disciplinari i dati relativi a conversazioni effettuate attraverso un'applicazione di messaggistica istantanea, estratti da uno smartphone in uso ad un lavoratore, in violazione dell'art. 4 della l. n. 300/1970, nonché della normativa in materia di *Privacy*, non potendo tale strumento essere ritenuto incluso nell'art. 4, secondo comma, della l. n. 300/1970, in mancanza di un vincolo di strumentalità tra tale applicativo e lo svolgimento della prestazione lavorativa da parte del dipendente (Tribunale - Milano, 24/10/2017).

Considerata da altra prospettiva, la questione è stata affrontata anche dal Garante per la protezione dei dati personali, il quale, nel provvedimento [https://www.lavorodirittieuropa.it/images/Garante privacy n. 243 del 18 aprile 2018.pdf](https://www.lavorodirittieuropa.it/images/Garante_privacy_n.243_del_18_aprile_2018.pdf), a fronte di una richiesta di blocco di un illegittimo trattamento di dati, ha considerato evidente “*come l'ordinamento non possa in alcun modo riconoscere, in presenza di un trattamento ritenuto non conforme alla disciplina in materia di protezione dei dati personali, l'eventualità di proseguire nel trattamento in questione e, conseguentemente, nella realizzazione dell'illecito, per soddisfare le esigenze giudiziarie del titolare del trattamento*”.

Come si può constatare:

a) abbiamo decisioni che si soffermano sull'onere di trasparenza a carico del datore di lavoro;

- b) altre decisioni citano, senza dettagli, la condizione del rispetto della *Privacy* quale condizione necessaria per l'utilizzo processuale di alcune informazioni;
- c) una decisione del Garante ostativa al trattamento dei dati “*per soddisfare esigenze giudiziarie*”.

4. LE POSSIBILI SOLUZIONI

La possibile soluzione alla precarietà delle disposizioni analizzate passa attraverso la delimitazione dell'ambito di applicazione dell'ultimo comma dell'art. 4 dello Statuto dei lavoratori.

Posto che il trattamento per fine di giustizia non può essere annichilito dalla disciplina della *Privacy* (art. 160-bis), la medesima disciplina della *Privacy* ha valore integrativo e non abrogativo delle norme processuali dettate a perimetrazione delle regole di giudizio a riguardo dell'ammissibilità delle prove.

Si parta dalla considerazione che, alla luce delle applicazioni giurisprudenziali sopra descritte, l'utilizzo di dati a tutti i fini del rapporto di lavoro comprende necessariamente l'utilizzo in sede processuale.

Si consideri, poi, che, per ovvie esigenze del “giusto processo”, la possibilità di utilizzo di fonti di prova in sede processuale deve essere prevedibile da parte di coloro che saranno parte del processo.

Si aggiunga, inoltre, che le disposizioni sulla possibilità di utilizzo dei dati in sede processuale devono essere ragionevoli (pena violazione dell'art. 3 della Costituzione).

È del tutto evidente, infatti, che una restrizione o un allargamento della possibilità di utilizzo processuali di fonte di prova ha dirette conseguenze sul rapporto sostanziale.

Quanto finora affermato, comunque, non significa affatto che le disposizioni sul trattamento dei dati non possano integrare le regole sull'onere della prova.

Proprio per l'impatto sostanziale, peraltro, le regole sul trattamento di dati impattanti sull'onere della prova devono sottostare a principi di ragionevolezza, come imposto dai canoni costituzionali.

Alla luce di quanto sopra, si ritiene che:

- a) la subordinazione dell'utilizzo processuale di dati al rispetto della disciplina sulla *Privacy* non può riguardare quelle disposizioni della disciplina sulla *Privacy* non rilevanti rispetto al rapporto sostanziale (intercorrente tra lavoratori e datori di lavoro), quali ad esempio adempimenti organizzativi a carico del titolare del trattamento; pertanto la subordinazione dell'utilizzo processuale di dati al rispetto della disciplina sulla *Privacy* deve essere quindi limitata esclusivamente a quelle disposizioni della disciplina sulla *Privacy* rilevanti rispetto al rapporto sostanziale (intercorrente tra lavoratori e datori di lavoro);
- b) rientrano tra le disposizioni rilevanti le disposizioni sulle informative e sulla base giuridica così come sui principi e sui diritti spettanti al lavoratore in quanto interessato.