

Ministero Interno: circolare Prot. 300/A/4027/20/127/9 del 8.06.2020

11 Giugno 2020

Notificazione a mezzo posta elettronica certificata delle sanzioni amministrative per violazioni del Codice della Strada - ulteriori indicazioni operative a tutela della riservatezza dei dati personali.

Leggi: [Ministero Interno circolare Prot. 300-A-4027-20-127-9 del 8.06.2020](#)

Circolare Min. dell'Interno 300/ A/2623/20/115/28 del 02/04/2020

11 Giugno 2020

Oggetto: Sospensione dei termini di notificazione dei processi verbali, di esecuzione del pagamento in misura ridotta, di svolgimento di attività difensiva e per la presentazione di ricorsi giurisdizionali in favore delle famiglie, lavoratori e imprese, connessa all'emergenza epidemiologica da COVID-19, e ulteriori proroghe disposte con DPCM 1 aprile 2020.

Leggi: [Min_Interno_Circ_2020_04_02](#)

Circolare Prefettura di Udine su obbligatorietà della figura del Messo Comunale

11 Giugno 2020

E' uscita una circolare prefettizia che, seppure in modo confuso e impreciso, richiama l'obbligatorietà della figura del Messo Comunale; questo a seguito di una serie di decisioni adottate da alcuni Sindaci del Friuli Venezia Giulia di non effettuare più il servizio di notificazione.

Numerose sono le imprecisioni, in primis, paradossalmente la mancata citazione della norma di riferimento principale relativa al messo comunale (legge 265/1999 art. 10), quindi la confusione fra messo notificatore e messo comunale per non parlare dell'indicazione del Sindaco ai fini della nomina a messo notificatore.

Leggi: [Circolare Prefettura di Udine obbligatorietà della figura del Messo Comunale](#)

Codice dei Contratti pubblici: i chiarimenti dell'ANAC sugli acquisti di importo inferiore ad € 1.000

11 Giugno 2020

L'Autorità Nazionale anti corruzione con [comunicato del Presidente del 30.11.2018](#) pubblicato sul sito istituzionale in data 12.11-2018 ha reso noto che sono giunte richieste di chiarimento in merito all'applicabilità dell'art.40, comma 2, del Codice dei contratti pubblici agli acquisti di importo inferiore a 1.000 euro.

In particolare, è stato chiesto se, in relazione alla disposizione recata dall'art. 40, co. 2 del Codice, sia consentito, per gli affidamenti infra 1.000 euro, procedere senza utilizzare mezzi telematici, in attuazione di quanto previsto dall'art. 1, co. 450 della legge 27 dicembre 2006, n. 296.

L'Autorità ritiene che, per gli acquisti infra 1.000 euro, permanga la possibilità di procedere senza l'acquisizione di comunicazioni telematiche, in forza della disposizione normativa da ultimo citata, non abrogata a seguito dell'emanazione del Codice dei contratti pubblici.

Legge 27/12/2006 n. 296

AMMINISTRAZIONE DEL PATRIMONIO E CONTABILITÀ DELLO STATO

Art. 1, co. 450

Le amministrazioni statali centrali e periferiche, ad esclusione degli istituti e delle scuole di ogni ordine e grado, delle istituzioni educative e delle istituzioni universitarie, nonché gli enti nazionali di previdenza e assistenza sociale pubblici e le agenzie fiscali di cui al decreto legislativo 30 luglio 1999, n. 300, per gli acquisti di beni e servizi di importo di importo pari o superiore a 1.000 euro e al di sotto della soglia di rilievo comunitario, sono tenute a fare ricorso al mercato elettronico della pubblica amministrazione di cui all'articolo 328, comma 1, del regolamento di cui al decreto del Presidente della Repubblica 5 ottobre 2010, n. 207. Fermi restando gli obblighi e le facoltà previsti al comma 449 del presente articolo, le altre amministrazioni pubbliche di cui all'articolo 1 del decreto legislativo 30 marzo 2001, n. 165, nonché le autorità indipendenti, per gli acquisti di beni e servizi di importo pari o superiore a 1.000 euro e inferiore alla soglia di rilievo comunitario sono tenute a fare ricorso al mercato elettronico della pubblica amministrazione ovvero ad altri mercati elettronici istituiti ai sensi del medesimo articolo 328 ovvero al sistema telematico messo a disposizione dalla centrale regionale di riferimento per lo svolgimento delle relative procedure. Per gli istituti e le scuole di ogni ordine e grado, le istituzioni educative, tenendo conto delle rispettive specificità, sono definite, con decreto del Ministro dell'istruzione, dell'università e della ricerca, linee guida indirizzate alla razionalizzazione e al coordinamento degli acquisti di beni e servizi omogenei per natura merceologica tra più istituzioni, avvalendosi delle procedure di cui al presente comma. A decorrere dal 2014 i risultati conseguiti dalle singole istituzioni sono presi in considerazione ai fini della distribuzione delle risorse per il funzionamento (215) (216).

(215) Comma così modificato dal comma 2 dell'art. 7, D.L. 7 maggio 2012, n. 52, come sostituito dalla legge di conversione 6 luglio 2012, n. 94, dai nn. 1) e 2) della lettera a) e dalla lettera b) del

comma 149 dell'art. 1, L. 24 dicembre 2012, n. 228, a decorrere dal 1° gennaio 2013, ai sensi di quanto disposto dall'art. 1, comma 561, della medesima legge n. 228/2012, dalla lettera b) del comma 8 dell'art. 22, D.L. 24 giugno 2014, n. 90, dall'art. 1, commi 495, lett. b), e 502, lett. a), b) e c), L. 28 dicembre 2015, n. 208, a decorrere dal 1° gennaio 2016, e, successivamente, dall'art. 1, comma 1, D.Lgs. 22 gennaio 2016, n. 10, a decorrere dal 29 gennaio 2016, ai sensi di quanto disposto dall'art. 3, comma 1 del medesimo D.Lgs. n. 10/2016. Vedi, anche, il comma 3-bis dell'art. 5, D.Lgs. 7 marzo 2005, n. 82, aggiunto dal comma 1 dell'art. 15, D.L. 18 ottobre 2012, n. 179, come modificato dalla legge di conversione 17 dicembre 2012, n. 221.

(216) Sull'applicabilità delle disposizioni di cui al primo periodo del presente comma vedi l'art. 10, comma 3, D.Lgs. 25 novembre 2016, n. 218.

A.N.A.C. : Comunicato del Presidente del 30 ottobre 2018

11 Giugno 2020

[Com.pres.30.10.2018 acquisti di importo inferiore a 1.000 euro](#)

Agenzia per l'Italia Digitale: Circolare 66 del 4 settembre 2014

11 Giugno 2020

[circolare_n._66_del_4_settembre_2014](#)

ANAC: Delibera n. 50/2013

11 Giugno 2020

Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016

Leggi: [ANAC Delibera-n.-50_2013](#)

Notifica all'estero di atti giudiziari ed extragiudiziari

11 Giugno 2020

Ministero degli Affari Esteri

Notifica all'estero di atti giudiziari ed extragiudiziari

L'attività di notificazione è una fase fondamentale dei processi civili, penali, tributari, amministrativi, fallimentari e del lavoro, nonché di alcune fasi pre-processuali o amministrative, che dà la conoscenza legale di un provvedimento mediante la consegna di un atto, giudiziario o extragiudiziario, da parte di un particolare soggetto notificatore, secondo precise modalità.

Ai sensi dell'art. 37 del D.Lgs. 71/2011 l'Ufficio consolare provvede alla notifica degli atti ad esso rimessi, in conformità alle disposizioni di cooperazione giudiziaria dell'UE, alle convenzioni internazionali in materia e alle leggi dello Stato di residenza.

NOTIFICA ALL'ESTERO DEGLI ATTI GIUDIZIARI ED EXTRAGIUDIZIARI IN MATERIA CIVILE E COMMERCIALE.

Le informazioni sono reperibili nella ["Guida alla notifica all'estero degli atti giudiziari ed extragiudiziari in materia civile e commerciale"](#).

NOTIFICA DI ATTI AMMINISTRATIVI A PERSONE RESIDENTI ALL'ESTERO

A. IN CASO DI INDIRIZZO CONOSCIUTO

1. La prima cosa da verificare è se il paese di destinazione abbia ratificato la convenzione di Strasburgo del 24.11.1977. Attualmente i paesi che hanno aderito sono **AUSTRIA, BELGIO, ESTONIA, FRANCIA, GERMANIA, ITALIA, LUSSEMBURGO** e SPAGNA* (le Autorità spagnole considerano che la Convenzione di Strasburgo del 1977 non sia applicabile ai casi di infrazioni la cui sanzione non rientri nella competenza delle Autorità giudiziarie, come nella maggior parte delle infrazioni stradali).

Tutte le informazioni riguardanti la Convenzione sono reperibili sul sito www.conventions.coe.int. Sotto il titolo "**Council of Europe Treaties**" che appare in alto a sinistra, cliccando sulla voce "**Full List**" si ha l'elenco completo delle convenzioni; quella che interessa la materia in questione è la **094 "European Convention on the Service abroad of Documents relating to Administrative Matters"**. Cliccando su questa voce, è possibile ottenere il testo della Convenzione (sia in formato Word che Html) nonché l'elenco delle Autorità Centrali designate dai Paesi aderenti per la ricezione delle notifiche ed i formulari da utilizzare (questi ultimi sono alla fine del testo della Convenzione in formato Word).

Ai sensi di tale Convenzione le richieste di notifica dovranno essere inviate:

- **direttamente alle Autorità** centrali designate dai paesi aderenti (in Italia al Ministero degli Affari Esteri). L'atto da notificare dovrà essere inviato in doppia copia, in lingua italiana (anche se si consiglia la traduzione nella lingua del paese destinatario o nella lingua veicolare conosciuta) accompagnato dal formulario;

oppure

- **ai sensi dell'art. 11, direttamente agli interessati dei provvedimenti a mezzo raccomandata con ricevuta di ritorno.** Alle modalità di notifica di cui all'art. 11 si oppone però la Germania.

2. Nel caso in cui il Paese non sia firmatario della predetta Convenzione (ma rientri nella lista di Paesi sottoriportata), è comunque possibile la **notifica a mezzo posta raccomandata** dal momento che la normativa locale non prevede motivi ostativi alla trasmissione diretta da parte degli uffici dell'Amministrazione pubblica italiana:

- ALBANIA
- AUSTRALIA
- CANADA
- CILE
- COLOMBIA
- COSTA RICA
- EL SALVADOR
- FILIPPINE
- FINLANDIA
- GIORDANIA
- GRAN BRETAGNA
- IRAQ
- IRLANDA
- ISRAELE
- LETTONIA
- MOZAMBICO
- NUOVA ZELANDA
- OMAN
- PAESI BASSI
- PARAGUAY
- PERU'
- PORTOGALLO
- REP. DI COREA
- SINGAPORE
- SLOVACCHIA
- SVEZIA
- UGANDA
- UNGHERIA

3. La notifica di atti a soggetti residenti nelle **Repubbliche della ex Jugoslavia (Bosnia-Erzegovina, Croazia, Macedonia, Montenegro, Serbia, Slovenia)** deve avvenire, come previsto dall'art. 4 della Convenzione italo-jugoslava di assistenza giudiziaria e amministrativa firmata a Roma il 3.12.1960, per il tramite del nostro Ministero della Giustizia. Gli atti andranno pertanto inviati direttamente al predetto Dicastero - DGGC Uff. II, Via Arenula 70, 00186 ROMA.

4. **Per tutti gli altri Paesi** l'atto, in doppia copia e con traduzione nella lingua del paese di destinazione o nella lingua veicolare in uso, va spedito direttamente alle Rappresentanze diplomatico-consolari italiane all'estero (il cui elenco è disponibile all'indirizzo <http://www.esteri.it/MAE/IT/Ministero/LaReteDiplomatica/Ambasciate/default.htm>). Sarà cura della Rappresentanza restituire all'ufficio richiedente una copia dell'atto con la relata di notifica.

B. IN CASO DI INDIRIZZO SCONOSCIUTO

Non è possibile effettuare la notifica dell'atto all'estero.

Normativa

- Codice di Procedura Civile, artt. 142, 143.
- [Convenzione dell'Aja del 1° marzo 1954 relativa alla procedura civile.](#)
- [Convenzione dell'Aja del 15 novembre 1965](#)
- [Regolamento \(CE\) n. 1393 del 13.11.2007 \(in vigore dal 13.11.2008\)](#), relativo alla notificazione e alla comunicazione negli Stati membri degli atti giudiziari ed extragiudiziali in materia civile o commerciale.
- Decreto Legislativo 3 febbraio 2011, n. 71 - Ordinamento e funzioni degli Uffici consolari.
- Convenzioni bilaterali, ove applicabili
- [Guida alla notifica all'estero degli atti giudiziari ed extragiudiziali in materia civile e commerciale](#)

Lavoro: le linee guida del Garante per posta elettronica e internet

11 Giugno 2020

Gazzetta Ufficiale n. 58 del 10 marzo 2007

Registro delle deliberazioni
Del. n. 13 del 1° marzo 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;

Vista la documentazione in atti;

Visti gli artt. 24 e 154, comma 1, lett. b) e c) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. Premessa

Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o 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.

Occorre muovere da alcune premesse:

- a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);
- c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
- d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
- e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili. (1)

1.2. Tutela del lavoratore

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. (2)

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato). (3)

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. Principi generali

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del

Codice). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. Discipline di settore

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (art. 47, comma 3, lett. b) Codice dell'amministrazione digitale). (4)

2.3. Principi del Codice

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

- a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2);
- b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3);
- c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, cit., punti 5 e 12).

3. Controlli e correttezza nel trattamento

3.1. Disciplina interna

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori; allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori"). (5)

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. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. Linee guida

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.

A seconda dei casi andrebbe ad esempio specificato:

se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna;
in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime -specifiche e non generiche- per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. Informativa (art. 13 del Codice)

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.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli. (6)

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire -a volte anche minuziosamente- l'attività di lavoratori. È il caso, ad esempio:

della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
dell'analisi occulta di computer portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. (7) A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice). (8)

5. Programmi che consentono controlli "indiretti"

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. (9) Ciò, anche in presenza di attività di controllo discontinue. (10)

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati (11), nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. (12)

5.2. Principio di necessità

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori (artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4).

Dal punto di vista organizzativo è quindi opportuno che:

si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature

suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
si individuino preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet; (13)

si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (c.d. privacy enhancing technologies-PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Prov. 2 febbraio 2006, cit.).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;

configurazione di sistemi o utilizzo di filtri che prevenivano determinate operazioni -reputate inconferenti con l'attività lavorativa- quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);

trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);

eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica

Il contenuto dei messaggi di posta elettronica -come pure i dati esteriori delle comunicazioni e i file allegati- riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale). (14)

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore

di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").

È quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);

il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; (15)

il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;

in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

6. Pertinenza e non eccedenza

6.1. Graduazione dei controlli

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. Conservazione

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario -e predeterminato- a raggiungerla (v. art. 11, comma 1, lett. e), del Codice).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

ad esigenze tecniche o di sicurezza del tutto particolari;

all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. Datori di lavoro privati

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (v., in particolare, art. 4, secondo comma, dello Statuto), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24, comma 1, lett. f) del Codice);

b) in caso di valida manifestazione di un libero consenso;

c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione

del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. Datori di lavoro pubblici

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (art. 29 del Codice).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9).

TUTTO CIÒ PREMESSO IL GARANTE

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);

b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:

si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;

si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;

si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi

abusivi;

c) l'adozione di misure di tipo tecnologico, e segnatamente:

I. rispetto alla "navigazione" in Internet (punto 5.2., a):

l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;

l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;

la graduazione dei controlli (punto 6.1.);

II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):

la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;

l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;

la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;

consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;

la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

d) l'analisi occulta di computer portatili affidati in uso;

4) individua, ai sensi dell'art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica

italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 1° marzo 2007

IL PRESIDENTE

Pizzetti

IL RELATORE

Paissan

IL SEGRETARIO GENERALE

Buttarelli

Ministero interno - Circolare n.7/92 del 4 luglio 1992

11 Giugno 2020

Messi notificatori e operatori di polizia municipale

Indirizzi omessi.

Sono pervenute a questo Ministero da parte delle associazioni rappresentative del personale della polizia municipale numerose richieste di intervento volte a far cessare l'espletamento delle mansioni di messo notificatore agli addetti al servizio di polizia municipale, in considerazione dell'incompatibilità delle medesime con quelle connesse alla figura professionale di vigile urbano.

La questione su esposta non è nuova a questo Ministero poiché è emersa in seguito all'entrata in vigore della legge-quadro 7 marzo 1986, n. 65, che, nel ridefinire il ruolo della polizia municipale, ha attribuito agli addetti al servizio l'esercizio anche delle funzioni ausiliarie di pubblica sicurezza per le quali è conferita loro, con decreto prefettizio, la qualità di agente di pubblica sicurezza.

In più occasioni questo dicastero direttamente interessato, si è espresso nel senso che il personale appartenente alla polizia municipale non è tenuto a svolgere le mansioni di messo notificatore atteso che tali mansioni, in base alle declaratorie di cui all'allegato A) al decreto del Presidente della Repubblica 25 giugno 1983, n. 347, si riferiscono ai dipendenti comunali appartenenti alla quarta e non alla quinta qualifica funzionale nella quale sono inquadrati i vigili urbani.

Tuttavia, non può sottacersi che l'assenza di una precisa descrizione dei profili professionali di ciascuna categoria del personale degli enti locali ha indotto le amministrazioni ad indugiare sulla applicazione della normative richiamata e ciò è avvenuto in particolare nei comuni di minori dimensioni che soggiacciono più di altri alle difficoltà derivanti dalla vigente normative in tema di provvista di mezzi finanziari da destinare a nuove assunzioni.

Ciò posto, si rileva che la questione in argomento ha trovato definitiva soluzione con l'entrata in vigore della legge 8 giugno 1990, n. 142, concernente il nuovo ordinamento delle autonomie locali il cui art. 64 ha abrogato, come è noto, l'art. 273 del T.U.L.C.P. n. 383/1934 che attribuiva al prefetto

l'emanazione del decreto di nomina a messo notificatore sia in capo ai vigili urbani che ad altro personale comunale.

Per effetto di tale abrogazione si ritiene che i decreti prefettizi di nomina, emessi prima dell'entrata in vigore della citata legge n. 142/1990, non possano più legittimare l'esercizio delle funzioni di messo notificatore per alcuno dei dipendenti delle amministrazioni comunali e conseguentemente tali funzioni debbono considerarsi definitivamente cessate, fatte salve le competenze delle regioni a statuto speciale e delle province autonome di Trento e Bolzano.

Si è dell'avviso, altresì, che la materia debba costituire oggetto delle norme statutarie degli enti stessi e che nelle more della sua definizione in sede di statuto, qualora si rendesse necessario notificare degli atti, sia il sindaco ad individuare i dipendenti comunali di quarta qualifica funzionale ai quali affidare l'incarico di messo notificatore, secondo le indicazioni già fornite al riguardo con circolare telegrafica di questo Ministero - Direzione centrale delle autonomie, prot. 98/L bis - L - 142/90, in data 7 febbraio 1992.