



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Ordinanza ingiunzione nei confronti di TPER Trasporto Passeggeri Emilia Romagna S.p.A. - 28 ottobre 2021 [9722661]

[VEDI ANCHE NEWSLETTER DEL 3 DICEMBRE 2021](#)

[doc. web n. 9722661]

**Ordinanza ingiunzione nei confronti di TPER Trasporto Passeggeri Emilia Romagna S.p.A. -
28 ottobre 2021**

Registro dei provvedimenti
n. 384 del 28 ottobre 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

RELATORE il prof. Pasquale Stanzone;

PREMESSO

1. Il reclamo.

Con specifico reclamo un dipendente della società Trasporto Passeggeri Emilia Romagna S.p.A. (di seguito "TPER" o la "Società") ha rappresentato profili di possibile violazione della disciplina di protezione dei dati personali nonché della disciplina di settore in materia di controlli a distanza dei lavoratori (artt. 114 del Codice in riferimento all'art. 4 l. 20 maggio 1970 n. 300, come modificato dall'art. 23 del d.lgs. 14 settembre 2015, n. 151). In particolare sono state lamentate presunte violazioni con riguardo al trattamento dei dati personali degli operatori addetti al call center posti in essere dalla Società mediante il sistema di gestione delle telefonate utilizzato per il servizio di assistenza all'utenza (call center inbound), mediante piattaforma dedicata "Phones", realizzata e fornita da IFM Infomaster S.p.A. (che svolgeva anche attività di manutenzione sulla piattaforma), in qualità di responsabile del trattamento (art. 28 del Regolamento; cfr. nota XX e relativi allegati, in atti).

2. L'attività istruttoria.

In riscontro alle specifiche richieste dell'Ufficio, la Società, azienda a totale partecipazione pubblica, affidataria del servizio di trasporto pubblico locale di Bologna e Ferrara, e di altri servizi (tra i quali il controllo sosta e rilascio contrassegni nel territorio del Comune di Bologna), che conta circa 2.500 dipendenti, ha dichiarato che (cfr., nota del XX, in atti):

- "il call center aziendale è uno dei canali principali per la diffusione delle informazioni all'utenza (come richiesto esplicitamente dall'art. 15 del Contratto di Servizio [...])" e "la Direttiva del Presidente del Consiglio dei Ministri 27 gennaio 1994, prevede che "i soggetti erogatori assicurano la piena informazione degli utenti circa le modalità di prestazione dei servizi" e "predispongono appositi strumenti di informazione, tramite l'attivazione di linee di comunicazione telefoniche e telematiche, cui verificano periodicamente il buon funzionamento (art 3, lett. e)";
- "il Contratto di servizio per l'affidamento del servizio automobilistico nel bacino di Bologna prevede, ad esempio, all'art. 14 comma 1 [che] "il concessionario è tenuto a dotarsi di un sistema di monitoraggio e rendicontazione del servizio erogato [...] finalizzato all'individuazione di misure preventive e correttive da porre in essere per garantire il costante adeguamento quantitativo e qualitativo del servizio alle esigenze dell'utenza anche potenziale";
- "l'attivazione delle registrazioni delle telefonate è quindi finalizzata al puntuale adempimento delle previsioni normative e dei vincoli contrattuali [...ed a] dirimere eventuali contenziosi (anche a garanzia dei lavoratori) e per consentire la verifica della piena correttezza delle operazioni effettuate";
- "per garantire la "riconoscibilità" e "rintracciabilità" degli operatori [...] il sistema all'inizio della telefonata comunica all'utente il numero di matricola identificativo dell'operatore";
- "il sistema telefonico utilizzato dagli addetti costituisce strumento di lavoro ai sensi dell'articolo 4 delta legge 300/70, come modificato dall'articolo 23 del d.lgs. 14.9.2015 n. 151 [pertanto...] la registrazione delle telefonate intercorse tra utenza e operatori di call center è consentita senza necessità di sottoscrizione di un previo accordo sindacale né della previa autorizzazione dell'INL [...] essendo sufficiente adeguata informativa, che è stata predisposta e fornita in formato cartaceo al personale interessato prima di attivare il sistema di registrazione telefonica [in ogni caso...] le OOSS [...] sono state preventivamente informate [...]. Il testo dell'informativa è stato anche affisso nei locali del call center aziendale";

- “l’attività di reportistica dei dati è effettuata in forma aggregata (non nominativa) per [...] adeguare il servizio offerto alle esigenze dei cittadini (giorni e fasce orario di picco); ripartire le telefonate per tipologia di servizio (servizi automobilistici, ferroviari, sosta, car sharing); ottemperare agli obblighi di reportistica previsti dal contratto di servizio (dati generici sul numero delle chiamate offerte/risposte e sulla tempistica delle risposte)”;
- l’addetto al call center accede “con le proprie credenziali aziendali personali [...] alla postazione di call center [...] compost[a] da un pc con installato un prodotto commerciale di IFM Infomaster Spa che effettua la gestione della conversazione telefonica e relativ[a] memorizzazione ed archiviazione [...]”;
- “la registrazione delle conversazioni telefoniche viene avviata automaticamente, senza alcuna opzione di scelta né da parte dell’utente né da parte dell’operatore dei call center: al termine della conversazione, la registrazione viene salvata automaticamente in modalità crittografata su una cartella di rete alla quale non è possibile accedere senza privilegi amministrativi. Non è possibile riascoltare una conversazione telefonica senza utilizzare l’apposita applicazione, alla quale si accede mediante apposite credenziali fornite alle sole persone autorizzate specificate nell’istruzione operativa aziendale IQC02 02”;
- “la conservazione delle registrazioni delle conversazioni telefoniche viene mantenuta, per policy aziendale, per un periodo pari a 3 (tre) mesi: al termine di questo periodo l[a] registrazion[e] viene automaticamente cancellata”, ciò al fine di “dirimere eventuali contestazioni da parte degli utenti in relazione all’utilizzo di determinati servizi quali, ad esempio, le operazioni eseguite con utilizzo di carta di credito”;
- “la piattaforma software che effettua la gestione della conversazione telefonica [...] contiene sempre e solo dati statistici raggruppati, che non consentono in alcun modo di risalire all’operatore che ha ricevuto la singola telefonata”;
- “per ogni singolo accesso deve essere tempestivamente fatta una registrazione nel Registro accesso file call center, che riporterà le informazioni previste dall’istruzione operativa aziendale IQC02 02”;
- “la procedura di ascolto della conversazione può essere attivata su richiesta motivata del singolo operatore [...]; su richiesta del Cittadino/utente [...]; da parte della società, nel caso di reclami motivati dettagliatamente da parte dei cittadini/utenti per verificare la corrispondenza di quanto segnalato; su istanza della pubblica autorità nell’ambito di procedimenti di competenza; a campione, su iniziativa aziendale, per verificare lo standard qualitativo del servizio con l’immediata cancellazione del dato, qualora non critico”;
- “in caso di accesso alla registrazione, la procedura prevede che questa venga spostata in altra directory e conservata a cura dei Responsabili indicati dalla procedura fino al termine della necessità di conservazione”;
- “finite le esigenze, fino a ipotetiche cause concluse, la registrazione sarà cancellata”.

In seguito, al fine di completare il quadro istruttorio con particolare riguardo al funzionamento del sistema, l’Ufficio ha condotto un’attività di accertamento, ai sensi dell’art. 58 del Regolamento e 157 e 158 del Codice, nei confronti della Società (cfr. verbale delle operazioni compiute del XX, in atti), nel corso del quale è stato dichiarato che:

- la Società “ha sempre effettuato il monitoraggio del servizio dapprima attraverso indagini statistiche, passando nel settembre 2018 alla registrazione delle telefonate, in ottica di garantire una migliore qualità del servizio [...]”;

- “la Società utilizza il call center inbound da molti anni, attraverso un numero unico 051290290, per la gestione dei rapporti con la clientela dei seguenti servizi: trasporto pubblico su gomma di Bologna e Ferrara, servizi ferroviari regionali gestiti da TPER, gestione dei contrassegni”;
- “il call center utilizza circa 20 dipendenti, suddivisi in 8 postazioni-operatore, coordinati da un responsabile [del servizio ...], inoltre, “oltre al personale in modalità stabile alla funzione di operatore di call center, vengono assegnati anche altri dipendenti temporaneamente non idonei alle mansioni per i quali sono stati assunti (ad esempio, autisti)”;
- “sulle circa 25.000 telefonate mensili verso il 051290290, vengono registrate circa 8.000 telefonate al mese, con picchi in alcuni periodi (ad esempio nel mese di ottobre 2019 sono state registrate circa 15.000 telefonate” (cfr. l’albero di navigazione IVR all. 2 al verbale);
- la società IFM S.p.A. di Genova, “designata Responsabile del trattamento, ha realizzato complessivamente la piattaforma di call center denominata “Phones” [...];
- la funzionalità di registrazione delle telefonate e cifratura dei file audio (RecReviewer) è aggiuntiva rispetto al pacchetto standard ed è stata acquisita con apposito atto integrativo” (cfr. all. 3 – verbale XX, copia del contratto con la società IFM);
- “gli utenti in grado di effettuare il riascolto delle telefonate, in ragione delle loro funzioni aziendali [...includono anche il], responsabile del call center”; tali soggetti seguono le specifiche procedure aziendali stabilite in proposito (cfr., all. 4 – verbale XX, copia della procedura aziendale IQC02_02 rev. 1);
- “i tecnici della società IFM non possono accedere ai dati delle registrazioni, conservati su infrastruttura TPER, se non per operazioni di manutenzione concordata tra le parti”;
- tali accessi [...] avvengono esclusivamente tramite VPN che viene aperta solo per l’effettuazione delle operazioni stesse e con accesso limitato e finalizzato [...e] non sono tracciate le operazioni effettuate dai tecnici di IFM sui dati conservati nella piattaforma Phones, mentre l’applicazione di riascolto delle telefonate prevede il tracciamento degli accessi e di alcune operazioni fra cui il riascolto delle telefonate” ma “la chiave di cifratura delle registrazioni è nota a IFM”.

Nel corso dell’accertamento in loco sono state verificate, tramite accesso alla piattaforma “Phones”, le funzionalità relative al riascolto delle chiamate (“RecReviewer”) e, all’esito degli accertamenti, è stato accertato che “nel database [erano] conservate le meta informazioni delle telefonate registrate, anche successivamente ai 90 giorni, e che tali meta informazioni comprendono il nome dell’operatore, la data e l’ora della chiamata e il numero di telefono chiamante. È stato altresì riscontrato che i primi dati disponibili risalgono a marzo 2018” (cfr. verbale XX, cit.).

Con nota del XX, a integrazione delle dichiarazioni rese nel corso dell’accertamento in loco, anche a scioglimento della riserva di produzione documentale avanzata nel contesto dell’attività ispettiva, la Società ha fatto pervenire ulteriori atti e documenti integrativi precisando, tra l’altro, che:

- il sistema “installato dal Fornitore e testato in TPER il XX (come da rapporto di intervento di IFM datato XX, doc. 4) [...] è stato attivato solo quasi 7 mesi dopo, ossia il XX, a seguito della conclusione delle approfondite analisi [e richiedendo] una valutazione legale ad un esperto giuslavorista circa le modalità di utilizzo dello strumento di RecReviewer. In sintesi, TPER ha chiesto conferma al proprio consulente di quali fossero le attività prodromiche da dover porre in essere a livello giuslavoristico, e una verifica del testo dell’informativa

destinata ai lavoratori TPER [...] Il legale ha confermato verbalmente alla Società che il software di registrazione delle telefonate in uso ad un call center potesse essere considerato uno strumento di lavoro [...] Tale analisi è stata ad oggi confermata dal consulente coinvolto” e dal “DPO [che ha effettuato la] valutazione d’impatto ai sensi dell’art. 35 del Regolamento UE 679/2016”;

- i dati raccolti tramite il sistema “non [sono] mai stat[i] utilizzat[i] da TPER per il monitoraggio dei lavoratori, tanto che nessuna sanzione disciplinare o nessuna premialità è stata irrogata/riconosciuta ai lavoratori da quando la Società ha attivato la registrazione delle chiamate degli operatori del call center”;

- sono stati convocati all’epoca “i sindacati per informarli dell’implementazione delle nuove funzionalità di cui trattasi e per condividere il testo dell’informativa privacy da rilasciare ai dipendenti interessati dal trattamento” (cfr. all. n. 2 e n. 3 nota del XX);

- successivamente all’attività istruttoria condotta dal Garante, TPER si è attivata “con il Fornitore per adeguare i sistemi informativi in modo che oltre alle registrazioni anche le meta-informazioni vengano cancellate dopo 90 giorni, fatta salva la facoltà di ulteriore conservazione per le suddette finalità (tutela in giudizio di TPER in caso di reclami, accesso agli atti da parte dei cittadini, adempimento di obblighi di legge o richieste di Autorità [precisando che] le meta-informazioni rinvenute nel corso dell’ispezione del XX, [...] si riferiscono ai test e alle attività svolte dal proprio fornitore IFM il XX al fine di verificare la configurazione del sistema di registrazione delle chiamate” (cfr. all. n. 4 nota XX).

Con nota del XX, l’Ufficio, sulla base degli elementi acquisiti, ha notificato alla Società, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, invitando il predetto titolare del trattamento a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall’Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24 novembre 1981).

Con la nota sopra menzionata, l’Ufficio ha rilevato che la Società ha posto in essere, mediante l’utilizzo del sistema (c.d. “Phones”), trattamenti di dati personali del reclamante e di altri dipendenti addetti al servizio di call center, in modo non conforme ai principi di “liceità, correttezza e trasparenza”, in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento, nonché in violazione degli artt. 6 e 88, par. 2 del Regolamento e dell’art. 114 del Codice, in relazione all’art. 4 della l. 20 maggio 1970, n. 300; in modo non conforme ai principi di “limitazione della finalità”, di “minimizzazione dei dati”, di “limitazione della conservazione”, nonché di “protezione dei dati personali fin dalla progettazione” e “per impostazione predefinita”, in violazione degli artt. 5, par. 1, lett. b), c) ed e), e 25 del Regolamento; in assenza di adeguate misure di sicurezza a tutela della integrità e riservatezza dei dati, in violazione degli artt. 5, par.1, lett. f) e 32 del Regolamento.

Con nota del XX la Società ha fatto pervenire le proprie memorie difensive, allegando la documentazione necessaria a comprovare le misure adottate con riguardo ai trattamenti in corso nei confronti dei dipendenti, e precisando, tra l’altro, che:

- nel contratto di servizio con l’ente pubblico concedente è previsto che “l’affidatario è tenuto a dotarsi di un sistema per il monitoraggio e la rendicontazione della qualità del servizio erogato (art. 14), e l’obbligo di garantire l’informazione all’utenza sul servizio offerto [...] mediante l’organizzazione di un servizio di “call-center”, riferito al complesso dei servizi affidati, anche avvalendosi di strutture terze, raggiungibile via telefonia [...] per fornire informazioni all’utenza, raccogliere reclami, proposte e suggerimento sulla gestione del servizio” (art. 15). [...]”. È, inoltre, previsto l’obbligo di “trasmettere un rapporto mensile sul servizio erogato, il cui contenuto minimo deve includere [una] “statistica consuntiva e aggiornata dei parametri del call-center (chiamate ricevute, chiamate accettate, chiamate

accettate dopo coda, tempi medi di attesa e di conversazione)”;

- “al fine di poter adempiere a quanto sopra, TPER ha ritenuto pertanto necessario e doveroso attivare la specifica funzione di registrazione delle chiamate ricevute al call-center”;

- “la necessità della registrazione è stata poi avvertita anche in ragione dei nuovi servizi offerti ai cittadini, che includono pagamenti mediante carte di credito” [e come] “strumento volto alla stessa tutela dei lavoratori in modo da poter adeguatamente gestire reclami o contestazioni degli utenti che certamente possono avere ad oggetto l’operato del personale del call-center”;

- “TPER [...ha] agito con tutta la dovizia di cautele e nella legittima convinzione di utilizzare lo strumento in questione in modo lecito e di poter considerare il call-center quale strumento a disposizione del personale TPER per rendere la propria prestazione lavorativa”;

- “nel caso in cui questa valutazione fosse stata sottoposta comunque alla conclusione di un accordo con il sindacato, la sua mancata conclusione avrebbe compromesso l’erogazione di servizi alla collettività e determinato la violazione degli impegni assunti verso l’Ente Pubblico, o esposto la Società al rischio di incorrere nelle penali che il Contratto di servizi prevede anche in caso di ritardo nell’adempimento”;

- “l’operato di TPER [può] essere al massimo rimproverato in termini di involontaria e opinabile erronea interpretazione della norma di cui all’art. 4 dello Statuto dei Lavoratori ma giammai potrà essergli imputata una scelta preordinata funzionale ad ottenere il controllo e il monitoraggio dei propri lavoratori”;

- la Società “ha deciso di convocare le organizzazioni sindacali [...il] XX al fine di conformarsi alle indicazioni” del Garante, precisando di aver “avviato le necessarie procedure richieste dalla legge con i propri sindacati”;

- le “meta-informazioni rinvenute nell’applicativo nel corso dell’ispezione del XX, [...si riferivano] ai test e alle attività svolte dal proprio fornitore [...] il XX al fine di verificare la configurazione delle chiamate [, ed esse] erano presenti a causa di un bug di sistema che TPER ha chiesto a IFM di risolvere” [, essendo] “ad oggi, tali informazioni [...] conservate per 90 giorni, come pure le registrazioni telefoniche” (cfr. allegati nn. 3 e 4 screenshot della query eseguita sul data base e ticket verso IFM per la gestione e risoluzione di questo bug);

- con riguardo all’informativa agli interessati, la Società si è impegnata a integrare la stessa con riguardo ai profili che risultavano originariamente carenti o non chiari, precisando comunque che “i lavoratori sono stati informati mediante Informativa alle OOSS del XX — prot. XX”;

- “sul tempo di conservazione delle chiamate e relativi meta-dati delle registrazioni, TPER, previa opportune valutazioni interne, ha deciso di fissarlo in 90 giorni, ritenendo tale periodo di tempo congruo e non eccessivo rispetto alle finalità che persegue [...atteso che] i cittadini potrebbero esercitare il diritto di accesso agli atti in caso di contenzioni amministrativi per sanzioni derivanti dalla violazione del codice della strada rispetto, ad esempio, ai servizi di accesso ZTL gestiti anche mediante il call-center: tenuto conto del tempo di notifica dei verbali di tali sanzioni [...];

- in ogni caso “la conservazione dei dati per la gestione di eventuali reclami è assolutamente eventuale e subordinata alla ricezione di reclami o al verificarsi di circostanze concrete e determinate; circostanze che TPER andrà di volta in volta ad analizzare ed opportunamente valutare affinché anche il proprio diritto di difesa (verso l’utente e l’Ente Pubblico a cui deve rendicontare il lavoro svolto) non venga vanificato dalla cancellazione dei dati e delle

chiamate. Sul punto si precisa altresì che nella policy aziendale ("Istruzione Operativa per la gestione delle registrazioni delle telefonate al Call Center" (cfr. Doc. n. 7) si legge espressamente che "... per operare un restore selettivo sarà necessaria l'autorizzazione scritta della Direzione";

- rispetto alle misure tecniche la Società ha precisato che "il cambio password dopo il primo accesso non è eseguibile per ragioni tecniche del prodotto offerto da IFM; sul punto IFM ha riferito alla Società che sta per apportare tali sviluppi. In ogni caso, TPER precisa che durante la formazione erogata al proprio personale affronta il tema della gestione delle password e istruisce il personale affinché lo stesso proceda al cambio periodico delle password [...]";

- "l'operato dei tecnici IFM viene gestito e "controllato" in ragione del fatto che esso avviene mediante collegamento VPN con IP fisso e previa intesa tra le parti. Inoltre, si precisa che l'operato di IFM deve seguire le specifiche istruzioni della Società e gli accordi del contratto di fornitura, posto che IFM agisce in qualità di responsabile del trattamento. Tra l'altro TPER non ha contezza di essere soggetta a un obbligo che impone il tracciamento di tali attività, obblighi che sa bene essere espressamente previsti in altre ipotesi (come ad esempio rispetto alle operazioni bancarie). Non si ritiene quindi che vi sia un obbligo normativo espresso che impone a TPER tale tracciamento";

- in ogni caso "i log attività di creazione e cancellazione utenze sono ora attivi, come si evince da query su db" (si vedano gli screenshot che si allegano di tale query, doc. n.10);

- "sulla mancanza di un log di cancellazione, si precisa che le chiamate vengono criptate e che gli utenti privi di un profilo da "Amministratore" sul sistema IFM non possono compiere operazioni di cancellazione; nell'assenza di un obbligo normativo che impone espressamente il tracciamento di tali operazioni, TPER ha ritenuto di non procedere con l'implementazione di tale tracciamento, fermo restando che questa misura di sicurezza verrà presa in considerazione nelle valutazioni relative alla scelta del nuovo sistema e fornitore di call-center";

- in ogni caso "la violazione, se confermata, deve ritenersi circoscritta ad un numero molto esiguo di interessati; come detto, gli operatori addetti al call-center erano e sono circa una ventina";

- ad avviso della Società "il personale [...] è a conoscenza di tutti i trattamenti svolti mediante il call-center, compreso quello di registrazione delle chiamate [...] e comunque la Società "non ritiene di aver arrecato alcun danno agli interessati".

In data XX si è, inoltre, svolta l'audizione richiesta dalla Società, ai sensi dell'art. 166, comma 6, del Codice, in occasione della quale, nel confermare quanto già dichiarato in sede di memorie difensive, è stato rappresentato, tra l'altro, che:

- "la Società ha messo in atto alcune azioni correttive avviando il percorso di relazioni industriali per addivenire ad un accordo ex art. 4 l. 300/1970 per conformare i trattamenti alle indicazioni del Garante. La Società ha colto l'occasione per disciplinare in tale sede anche i trattamenti che si intende porre in essere mediante altre tecnologie [...] che potrebbero ricadere nell'ambito dell'art. 4 l. 300/1970";

- "il XX si è concluso in modo infruttuoso il percorso relativo alle relazioni industriali, l'accordo non è stato siglato, quindi si è provveduto a richiedere l'autorizzazione all'Ispektorato del lavoro territorialmente competente, procedimento che non si è ancora concluso";

- “allo stato il sistema di registrazione delle chiamate oggetto della presente istruttoria non è funzionante e tutti i dati e i metadati raccolti e memorizzati, ivi comprese le telefonate per le quali è stato effettuato il riascolto, sono stati cancellati e il trattamento è stato interrotto”;
- “il XX la Società ha aggiornato il testo [dell’informativa generale resa a tutti i dipendenti], condividendola con il personale, mentre quella specifica relativa ai trattamenti di dati del personale addetto al call center sarà aggiornata all’esito del procedimento autorizzatorio per poter tenere conto delle indicazioni dell’Ispettorato [...] [e] saranno altresì effettuati nuovi corsi di formazione alla luce delle nuove funzionalità che saranno implementate tenendo conto delle indicazioni del Garante e dell’Ispettorato”;
- “con riguardo alle chiamate in entrata sul call center è stata corretta l’informativa breve resa all’utenza nella quale non si dà più conto delle operazioni di registrazione, in quanto non più effettuate”.

3. Esito dell’attività istruttoria.

In base alla disciplina in materia di protezione dei dati personali, il datore di lavoro può trattare i dati personali, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1, del Regolamento), dei lavoratori se il trattamento è necessario, in generale, per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti dalla disciplina di settore (artt. 6, par. 1, lett. c), 9, par. 2, lett. b) e 4; 88 del Regolamento). Il trattamento è, inoltre, lecito quando sia “necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento” (artt. 6, par. 1, lett. e), 2 e 3 del Regolamento; 2-ter del Codice, nel testo anteriore alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, vigente all’epoca dei fatti oggetto dell’istruttoria).

Il datore di lavoro deve, inoltre, rispettare le norme nazionali, che “includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati in particolare per quanto riguarda la trasparenza del trattamento [...] e i sistemi di monitoraggio sul posto di lavoro” (artt. 6, par. 2, e 88, par. 2, del Regolamento). Sul punto il Codice, confermando l’impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro (artt. 113 “Raccolta dati e pertinenza” e 114 “Garanzie in materia di controllo a distanza”). Per effetto di tale rinvio, e tenuto conto dell’art. 88, par. 2, del Regolamento, l’osservanza degli artt. 4 e 8 della l. 20 maggio 1970, n. 300 e dell’art. 10 del d.lgs. n. 297/2003 (nei casi in cui ne ricorrono i presupposti) costituisce una condizione di liceità del trattamento.

Tali norme costituiscono nell’ordinamento interno quelle disposizioni più specifiche e di maggiore garanzia di cui all’art. 88 del Regolamento - a tal fine oggetto di specifica notifica dal Garante alla Commissione, ai sensi dell’art. 88, par. 3, del Regolamento - la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione - analogamente alle specifiche situazioni di trattamento del capo IX del Regolamento - determina anche l’applicazione di sanzioni amministrative pecuniarie ai sensi dell’art. 83, par. 5, lett. d), del Regolamento (cfr., con riguardo all’ambito lavorativo pubblico, da ultimo, provv. 22 luglio 2021, n. 273 doc. web n. [9683814](#), spec. par. 4 e provv. 13 maggio 2021, n. 190, doc. web n. [9669974](#); cfr., anche la giurisprudenza della Corte europea dei diritti dell’uomo, nel caso Antovic e Mirkovic v. Montenegro, application n. 70838/13 del 28.11.2017, che ha stabilito che il rispetto della “vita privata” deve essere esteso anche ai luoghi di lavoro pubblici, evidenziando che i controlli sul posto di lavoro possono essere effettuati solo nel rispetto delle garanzie previste dalla legge nazionale applicabile).

Il titolare del trattamento è, comunque, tenuto a rispettare i principi in materia di protezione dei dati (art. 5 del Regolamento) ed è responsabile dell’attuazione delle misure tecniche e organizzative

adeguate a garantire e essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento). I dati devono, inoltre, essere “trattati in maniera da garantire un’adeguata sicurezza” degli stessi, “compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali” (art. 5, par. 1, lett. f); v. anche art. 32 del Regolamento).

3.1. Il trattamento dei dati effettuato tramite il sistema di registrazione delle telefonate inbound “Phones”.

Dall'accertamento compiuto risulta che la Società aveva adottato, fin dal XX, un sistema per la gestione delle telefonate della clientela (call center inbound) che consentiva operazioni di trattamento di dati personali, riferiti al personale addetto al call center (o di altro personale impiegato in tale servizio a rotazione, che fosse impossibilitato a svolgere le ordinarie mansioni, es. autisti temporaneamente inidonei al servizio).

Allo stato, stando a quanto da ultimo dichiarato dalla Società, il sistema sarebbe stato disattivato (cfr. verbale audizione del XX).

In particolare il sistema di gestione delle chiamate in entrata della clientela (call center inbound), cui su richiesta della Società era stata aggiunta la funzionalità di registrazione delle telefonate, era stato realizzato, tramite la società IFM S.p.A. di Genova, fornitrice anche del servizio di manutenzione. Il sistema consentiva che una parte delle telefonate della clientela ricevute dagli operatori, identificati anche tramite il proprio numero di matricola, fosse automaticamente registrata sulla piattaforma denominata “Phones” e ivi memorizzate per tre mesi, previa cifratura dei file audio (funzionalità “RecReviewer” aggiuntiva rispetto al pacchetto standard offerto dal Fornitore).

Oltre alla specifica funzionalità di registrazione delle telefonate era prevista la possibilità di riascolto delle telefonate memorizzate, mediante una specifica procedura che poteva essere attivata dalla Società o su richiesta di un cittadino o un operatore, di regola, per la gestione di eventuali reclami, e “a campione, su iniziativa aziendale, per verificare lo standard qualitativo del servizio con l'immediata cancellazione del dato, qualora non critico” (cfr. verbale XX, cit.). Il riascolto della registrazione avveniva tramite apposita applicazione, alla quale si accedeva mediante credenziali fornite alle sole persone autorizzate (cfr. Istruzione operativa aziendale IQC02 02). La procedura prevedeva che la telefonata da riascoltare venisse spostata in altra directory e conservata a cura dei responsabili indicati dalla procedura fino al termine della necessità di conservazione (cfr. verbale del XX, cit.).

Il sistema consentiva inoltre l'estrazione di “reportistica dei dati in forma aggregata (non nominativa) per [...] ottemperare agli obblighi di reportistica previsti dal contratto di servizio (dati generici sul numero delle chiamate offerte/risposte e sulla tempistica delle risposte)” (cfr. verbale ispettivo del XX, cit.).

Come emerso nel corso delle verifiche effettuate mediante accesso diretto al sistema nel corso degli accertamenti ispettivi, il sistema consentiva altresì la raccolta e la conservazione delle meta informazioni relative alle chiamate registrate e, dunque, il trattamento di taluni dati personali riferiti ai dipendenti addetti al call center (quali, il nome dell'operatore, la data e l'ora della chiamata e il numero di telefono chiamante) con conservazione per un arco temporale che, all'epoca dell'accertamento compiuto, non era stato definito dalla Società (cfr. p. 9, verbale del XX).

3.2. Liceità correttezza e trasparenza: l'informativa ai dipendenti e le condizioni di liceità del trattamento.

Il titolare del trattamento deve trattare i dati “in modo lecito, corretto e trasparente nei confronti

dell'interessato" (art. 5, par. 1, lett. a) del Regolamento), adottando "misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 [...]" (art. 12 del Regolamento).

L'esame della informativa resa ai dipendenti ha messo in evidenza che la Società ha certamente informato il personale e, con separata comunicazione, anche le organizzazioni sindacali della definitiva attivazione dal XX di "un sistema di registrazione delle telefonate che intercorrono tra l'utenza e gli addetti, con possibilità di riascolto a campione delle telefonate, anche per dirimere eventuali contenziosi" (cfr. informativa in atti); tuttavia l'informativa non riportava tutte le informazioni richieste dall'art. 13 del Regolamento per assicurare un trattamento corretto e trasparente, quali, in particolare, l'indicazione dei diritti degli interessati di cui agli artt. 15-22 del Regolamento e il diritto di proporre reclamo all'autorità di controllo.

Inoltre, il documento si limitava a menzionare la funzionalità di registrazione delle chiamate rispetto alla quale si precisava che "i dati raccolti saranno conservati per il tempo strettamente necessario per assolvere le finalità indicate, ovvero 90 giorni salvo contenziosi da conservare fino a risoluzione" (cfr. informativa, in atti), senza invece far alcun riferimento alla raccolta e alla memorizzazione delle cc.dd. meta informazioni, riferite ai dipendenti e alla loro attività lavorativa, operazioni di trattamento rispetto alle quali, all'epoca delle verifiche, la Società non aveva peraltro stabilito un termine massimo di conservazione.

Sempre con riferimento alla trasparenza e correttezza del trattamento, si precisa che l'informativa espressamente menzionava che "il consenso al trattamento dei dati emergenti dalle registrazioni delle telefonate non è richiesto, in quanto finalizzato ad eseguire obblighi derivanti da un contratto di servizio del quale Tper è parte interessata". Se correttamente il testo escludeva il ricorso al consenso quale presupposto di liceità - atteso che il consenso dell'interessato non può, di regola, costituire un valido presupposto di liceità per il trattamento dei dati personali quando sussista "un evidente squilibrio tra l'interessato e il titolare" (cfr. considerando 43 del Regolamento), circostanza che ricorre in particolare nel contesto lavorativo (cfr., Comitato per la protezione dei dati, Linee Guida sul consenso ai sensi del Regolamento UE 2016/679- WP 259- del 4 maggio 2020, par.3.1.1.; v. anche Parere 2/2017 sul trattamento dei dati sul posto di lavoro, adottato dal Gruppo di lavoro art. 29 adottato l'8 giugno 2017, WP 249) – il riferimento al contratto, quale condizione di liceità del trattamento, non risulta pertinente nel caso di specie. L'espressione "necessario per l'esecuzione di un contratto" di cui all'art. 6, par. 1, lett. b) del Regolamento), si riferisce al caso in cui "il trattamento deve essere necessario per adempiere il contratto con ciascun interessato" e non invece come nel caso di specie nell'esecuzione di un contratto di servizio tra il titolare e un tezo, ente appaltante.ad esempio, con riguardo al contesto lavorativo, "questo presupposto potrebbe permettere, per esempio, il trattamento di informazioni riguardanti lo stipendio e le coordinate bancarie per consentire il pagamento degli stipendi" (cfr. parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato dal Gruppo di lavoro Articolo 29 il 9 aprile 2014, pagg. 19-20, WP 217). Come chiarito anche di recente dal Comitato per la protezione dei dati, infatti, "è necessario che vi sia un collegamento diretto e obiettivo tra il trattamento dei dati e la finalità dell'esecuzione del contratto con gli interessati" (cfr., Linee Guida sul consenso ai sensi del Regolamento UE 2016/679, cit.).

Il trattamento di dati dei dipendenti effettuato dalla Società mediante il sistema in esame, essendo invece finalizzato all'assistenza dell'utenza in vista del miglioramento della qualità e dell'efficienza del servizio di trasporto pubblico locale di cui la Società è concessionaria, può essere piuttosto considerato nell'ambito dell'esecuzione di un compito di interesse pubblico e degli obblighi previsti dalla disciplina di settore (art. 6, par.1, lett. e) del Regolamento). Stante, poi, la titolarità del trattamento dei dati dei propri dipendenti e collaboratori, per la gestione del rapporto di lavoro, il trattamento deve comunque essere effettuato anche nel quadro delle norme nazionali più specifiche che regolano l'impiego di strumenti tecnologici nel contesto lavorativo e che, come chiarito nel tempo dal Garante (cfr. par. 3 del presente provvedimento), costituiscono specifiche condizioni di liceità del trattamento (cfr., art. 5, 6 e 88 del Regolamento e 114 del Codice e art. 4, l.

20 maggio 1970, n. 300). A tale quadro normativo di settore fa, peraltro, rinvio la stessa Società nel testo dell'informativa originariamente resa ai dipendenti ove si legge che "Tper potrà utilizzare le informazioni e i dati raccolti tramite le registrazioni per tutti i fini connessi al rapporto di lavoro (ad es. per sistema premiante e disciplinare)", ipotesi espressamente prevista dall'art. 4, comma 3, l. n. 300/1970.

Per tali ragioni, il documento informativo originariamente messo a disposizione dei dipendenti non conteneva tutti gli elementi espressamente richiesti dal Regolamento, non forniva una chiara e trasparente rappresentazione del complessivo trattamento effettuato tramite il sistema "Phones" sia con riguardo ad alcune operazioni di trattamento (es. raccolta e memorizzazione delle meta informazioni) sia con riguardo ai presupposti di liceità dello stesso, in violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento.

Si dà tuttavia atto che nel corso del procedimento, la Società ha provveduto ad aggiornare il testo dell'informativa generale resa ai dipendenti, intervenendo "ulteriormente sul testo dell'informativa per renderla più trasparente e fruibile anche in merito alla base legale applicata ex art. 6 del GDPR", e riservandosi di predisporre una specifica relativa ai trattamenti di dati del personale addetto al call center "all'esito del procedimento autorizzatorio per poter tenere conto delle indicazioni dell'Ispettorato" (cfr. verbale audizione cit.).

3.3. La disciplina di settore in materia di controlli a distanza.

Come emerso nel corso dell'istruttoria il sistema era finalizzato, sulla base di specifici contratti di servizio, a migliorare e rendere efficiente la qualità del servizio reso nei rapporti con l'utenza, quindi funzionale a rispondere a esigenze di carattere organizzativo e produttivo, nonché di efficienza ed economicità dell'attività e del servizio pubblico erogato.

Nell'ambito degli accertamenti è stato verificato che, oltre a consentire la ricezione e gestione delle telefonate e trattare informazioni necessarie per rispondere alle richieste dell'utenza, il sistema rendeva possibili altre operazioni di trattamento di dati riferiti al personale impiegato presso il servizio di call center. Dalle verifiche effettuate sulle specifiche caratteristiche del sistema è, infatti, emerso che questo era dotato di funzionalità che permettevano anche la memorizzazione e riascolto delle telefonate, nonché la raccolta di informazioni di dettaglio (meta informazioni: il nome dell'operatore, il numero chiamante, la data e l'ora della chiamata – cfr. p. 9 del verbale del XX), associate in via diretta al dipendente che gestiva la telefonata con l'utente.

Nello specifico contesto, come detto (cfr. par. 3 e 3.1 del presente provvedimento) la liceità del trattamento è connessa anche all'osservanza della disciplina di settore in materia di impiego di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" (art. 5 e 6 par. 1, lett. c), e 88, par. 2, del Regolamento e 114 del Codice).

In questi anni il Garante, specie a seguito delle modifiche apportate alla l. 20 maggio 1970, n. 300, dall'art. 23 del d. lg. n. 151/2015, ha affrontato anche il tema del discrimine tra il comma 1 e il comma 2 dell'art. 4 della l. n. 300/1970 e del diverso regime giuridico che ne discende, valutando, di volta in volta, la specificità dei trattamenti e dei sistemi utilizzati in concreto dal datore di lavoro, tenendo conto degli orientamenti della giurisprudenza, del Ministero del lavoro e dell'Ispettorato Nazionale del lavoro, che applicano tale disciplina nell'ambito delle proprie funzioni istituzionali di controllo (cfr., tra i numerosi provvedimenti adottati, da ultimo, provv. 13 maggio 2021, n. 190, doc. web n. [9669974](#); provv. 13 luglio 2016, n. 303, par. 4.3, doc. web [5408460](#) e provv. 16 novembre 2017, n. 479, doc. web n. [7355533](#); Relazione annuale 2016, p. 100 e Relazione annuale 2017, p.115 ss.).

Con riguardo all'installazione e utilizzazione di strumenti di supporto all'attività ordinaria dei call center, l'Ispettorato nazionale del lavoro ha precisato che "possono essere considerati strumenti di

lavoro” (ai sensi dell’art. 4, comma 2 della l. n. 300/1970) i sistemi che “consentano il mero collegamento tra la chiamata e l’anagrafica del cliente senza ulteriori elaborazioni”, viceversa, negli altri casi, ad esempio quando consentano di effettuare anche “ulteriori elaborazioni”, essi sono comunque atti a realizzare un indiretto e preterintenzionale “monitoraggio dell’attività telefonica” effettuata dagli operatori addetti al call center con possibilità di ricostruirne anche indirettamente l’attività (cfr. INL, circolare n. XX del XX, che contiene indicazioni operative sull’installazione e utilizzazione di strumenti di supporto all’attività operativa ordinaria dei Call Center).

Tali strumenti che comportano “un controllo ‘incidentale’ sull’attività del lavoratore” rientrano, quindi, nell’ambito di applicazione dell’art. 4, comma 1, della l. n. 300/21970 (sempreché, precisa l’Ispettorato, non diano luogo a “controlli prolungati, costanti, indiscriminati e invasivi” nel qual caso “non si ravvisano neanche quelle esigenze organizzative e produttive che giustificano il rilascio del provvedimento autorizzativo da parte dell’Ispettorato del Lavoro”, cfr. INL, circolare n. XX del XX cit.).

In coerenza con tale orientamento, il Garante ha già adottato, nel recente passato, alcune specifiche decisioni nei confronti di operatori economici che impiegavano simili sistemi per la gestione dei rapporti con la clientela e per il miglioramento della qualità dei servizi offerti, aderendo a tale interpretazione (cfr., provv.ti nn. 139 dell’8 marzo 2018, doc. web n. [8163433](#) e 229 del XX, spec. par. 2 e 3, doc. web n. [8987133](#)).

Come verificato nel corso dell’istruttoria, il sistema impiegato dalla Società non si limitava a consentire l’associazione tra la chiamata in entrata e l’anagrafica del cliente per facilitare e semplificare l’attività dell’operatore di call center nella rapida ed efficiente gestione delle richieste dell’utenza, né consisteva in un mero archivio informatico a uso dei soli dipendenti che hanno rapporti con gli utenti, ma consentiva anche altre operazioni di trattamento e “ulteriori elaborazioni” e, nello specifico, la registrazione delle chiamate e la memorizzazione delle meta informazioni ad esse relative associate direttamente ai nominativi dei dipendenti che le avevano effettuate nell’ambito della propria attività lavorativa.

Alla luce delle considerazioni che precedono e delle descritte caratteristiche del sistema, che peraltro non consentivano di escludere la memorizzazione di informazioni associate in via diretta ai dipendenti (“la registrazione delle conversazioni telefoniche viene avviata automaticamente, senza alcuna opzione di scelta né da parte dell’utente né da parte dell’operatore dei call center”, cfr. nota XX e verbale accertamenti ispettivi, cit.), il perseguimento da parte della Società delle specifiche finalità (“organizzative e produttive”) mediante il predetto sistema avrebbe dovuto avvenire anche nel rispetto delle condizioni di garanzia prescritte dall’articolo 4, comma 1 della legge n. 300 del 1970 (accordo sindacale o, in alternativa, autorizzazione pubblica; cfr. sul punto INL, circolare n. XX del XX).

Contrariamente alle originarie valutazioni del titolare del trattamento - effettuate sulla base di pareri rilasciati da propri consulenti -, il citato sistema, alla luce del quadro normativo di settore e delle richiamate indicazioni rese nel tempo dal Garante, non può, infatti, essere considerato tra gli “strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa”, ai sensi e per gli effetti dell’art. 4, comma 2, l. n. 300/1970 rientrando piuttosto, anche per l’impossibilità per il singolo operatore di disattivare la funzione di memorizzazione, tra gli strumenti organizzativi di cui all’art. 4, comma 1, l. n. 300/1970.

Pertanto, se da un lato le finalità che la Società intendeva perseguire con il sistema di gestione delle telefonate in questione (ossia quello di garantire il costante adeguamento quantitativo e qualitativo del servizio alle esigenze dell’utenza) risultano riconducibili alle lecite “esigenze organizzative e produttive [...]”, espressamente fatte salve dal predetto articolo 4, comma 1, dall’altro la Società, non ha però attivato, essendovi tenuta, le garanzie procedurali prescritte dalla

medesima norma (accordo sindacale o autorizzazione all'Ispettorato nazionale del lavoro).

Considerato altresì che tali garanzie non possono essere soddisfatte con il mero invio alle organizzazioni sindacali di un documento informativo, come invece avvenuto nel caso di specie (si veda sul punto, provv. 17 dicembre 2020, n. 282, doc web n. [9525337](#), ma già provv. ti 13 luglio 2016, n. 303, par. 4.3, doc web [5408460](#) e 16 novembre 2017, n. 479, doc. web n. [7355533](#), par. 3.2.), il trattamento dei dati personali dei dipendenti, addetti al call center, effettuato dalla Società tramite il sistema “Phones” risulta avvenuto, fino alla disattivazione del sistema e alla interruzione del trattamento (cfr., verbale audizione del XX, cit.), in contrasto con la disciplina in materia di protezione dei dati personali e con la rilevante disciplina di settore, avendo la Società installato il medesimo senza attivare le procedure di garanzia previste dalla legge di settore applicabile (in violazione degli artt. 5, comma 1, lett. a); 6, comma 1, lett. c); 88 del Regolamento e 114 del Codice, in relazione all'art. 4 della l. 20 maggio 1970, n. 300).

3.4. Minimizzazione, protezione dei dati fin dalla progettazione e per impostazione predefinita, e limitazione della conservazione e della finalità.

In base al Regolamento, il trattamento deve avere ad oggetto i soli dati “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati” e la conservazione dei dati, in una forma che consenta l'identificazione degli interessati, è ammessa “per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattate” (art. 5, par. 1, lett. c) ed e) del Regolamento). Anche in considerazione del rischio che incombe sui diritti e le libertà degli interessati, il titolare del trattamento, in base ai principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del Regolamento; cfr. anche Considerando nn. 75 e 78), deve mettere in atto “misure tecniche e organizzative adeguate [...] volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del [...] regolamento e tutelare i diritti degli interessati” (par. 1).

Come risulta dalla complessiva attività istruttoria, il sistema consentiva, invece, la memorizzazione sistematica e la conservazione delle meta informazioni relative alle chiamate registrate per un tempo, alla data degli accertamenti, non ancora definito dal titolare (cfr. p. 9 verbale del XX dal quale risulta, infatti, che i dati presenti sul sistema erano risalenti al 2018).

Il titolare del trattamento, oltre a rispettare il principio della “protezione dei dati fin dalla progettazione” (art. 25, par. 1, del Regolamento) – adottando misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati – deve anche, in conformità al principio della “protezione dei dati per impostazione predefinita” (art. 25, par. 2, del Regolamento), effettuare scelte tali da garantire che venga effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire una specifica e lecita finalità. Ciò comporta che, per impostazione predefinita, il titolare del trattamento non deve raccogliere dati personali che non sono necessari per la specifica finalità del trattamento (cfr. “Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita”, adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 42, 44 e 49).

Come recentemente messo in evidenza dal Garante (cfr., con riguardo a specifici trattamenti in ambito lavorativo, provv. n. 235 del 10 giugno 2021, doc. web n. [9685922](#); ma v. con riguardo al trattamento di dati di utenti e dipendenti mediante un sistema di prenotazione di servizi allo sportello, provv. 17 dicembre 2020, n. 282, doc. web n. [9525337](#)), il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare, anche avvalendosi del supporto del Responsabile della protezione dei dati ove nominato, la conformità ai principi applicabili al trattamento dei dati (art. 5 del Regolamento) adottando, nel rispetto del principio di

responsabilizzazione, le opportune misure tecniche e organizzative e impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2, 24, 25 e 32 del Regolamento). In tale prospettiva, il titolare del trattamento deve accertarsi che siano disattivate, in particolare, le funzioni che non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento e, in particolare, con riguardo al caso di specie le norme nazionali e di maggior tutela per gli interessati con riguardo ai trattamenti in ambito lavorativo (art. 88 del Regolamento in relazione agli artt. 113 e 114 del Codice).

Per tali ragioni, tenuto conto delle rappresentate esigenze organizzative e di efficienza del servizio perseguite con il citato sistema, del quadro normativo di settore applicabile (art. 4, comma 1, l. n. 300/1970) e dell'orientamento del Garante in materia (cfr., provv. 16 novembre 2017, n. 479 doc. web n. [7355533](#), cit. e provvedimenti 22 dicembre 2016, n. 547, doc. web n. [5958296](#), par. 3.5 e 13 luglio 2016, n. 303, par. 5, cit.; ma v. anche Linee guida per posta elettronica e internet, provv. del 1° marzo 2007, n. 13, doc. web n. [1387522](#), spec. par. 4, con principi che possono ritenersi tutt'ora validi; più in generale, Consiglio di Europa, Raccomandazione del 1° aprile 2015, CM/Rec (2015)5, spec. princ. 14 -15 e Article 29 Working Party, Opinion 2/2017 on data processing at work, WP 249, par.5), le specifiche operazioni di trattamento consistenti nella raccolta e memorizzazione per un arco temporale indefinito delle meta informazioni riferite direttamente ai dipendenti e alla loro attività lavorativa, non risultano conformi ai principi di minimizzazione e di limitazione della conservazione dei dati nonché di protezione dei dati personali fin dalla progettazione e per impostazione predefinita, in violazione degli artt. 5, par. 1, lett. c) ed e), e 25 del Regolamento.

I descritti trattamenti non possono essere ritenuti giustificati neanche per le ulteriori finalità, legate all'utilizzo nell'ambito di eventuali reclami da parte di cittadini e utenti, pure invocate dalla Società e richiamate nell'informativa ai dipendenti. Il trattamento di dati personali effettuato per finalità di tutela dei diritti deve infatti riferirsi a contenziosi in atto o a situazioni precontenziose e non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (tale principio generale è stato, da ultimo, ribadito dal Garante proprio con riguardo al contesto lavorativo nel "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101", All. 1, par. 1.3, lett. d), doc. web n. [9124510](#)).

Stante, poi, il principio in base al quale i dati devono essere "raccolti per finalità determinate, esplicite legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" (art. 5, par. 1, lett. b) del Regolamento) si fa presente da ultimo che, sebbene la Società abbia dichiarato che i dati raccolti dal sistema non sono "mai stat[i] utilizzat[i] da TPER per il monitoraggio dei lavoratori, tanto che nessuna sanzione disciplinare o nessuna premialità è stata irrogata/riconosciuta ai lavoratori da quando la Società ha attivato la registrazione delle chiamate degli operatori del call center", nel corso dell'istruttoria è emerso che la stessa si era comunque riservata, in generale, la possibilità di utilizzare dei dati raccolti tramite il sistema per tutti i fini connessi alla gestione del rapporto di lavoro (art. 4, comma 3, l. n. 300/1970), come risulta dal testo dell'informativa in atti.

Al riguardo, sebbene non vi siano evidenze in atti di trattamenti effettuati da parte della Società per tali finalità (ragione per cui si ritiene di archiviare la contestazione in relazione a tale profilo), appare necessario chiarire che il quadro normativo vigente consente che i dati raccolti ai sensi dell'art. 4, commi 1 e 2 della legge n. 300/1970 possono 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).

Come recentemente messo in evidenza dal Garante con il provvedimento del 13 maggio 2021, n.

190, “il quadro normativo vigente consente al titolare (datore di lavoro) di utilizzare i dati identificativi dei lavoratori, per ulteriori finalità, nell’ambito della gestione del rapporto, solo le informazioni raccolte nel rispetto delle condizioni e dei limiti previsti dall’art. 4” della l. n. 300/1970 (nel caso di specie con riferimento al comma 1) e dunque “nei limiti in cui l’originaria raccolta sia stata ,lecitamente effettuata”. Tale quadro presuppone quindi un’autonoma determinazione del titolare circa l’utilizzazione delle informazioni, ove già lecitamente raccolte nel rispetto delle condizioni e dei limiti previsti dall’art. 4, commi 1 o 2 della l. n. 300/70, anche per ulteriori trattamenti necessari alla gestione del rapporto di lavoro (art. 4, comma 3 della l. 300/1970). Tali successive ed eventuali operazioni di trattamento presuppongono il rispetto del quadro normativo di riferimento sia in materia di controlli a distanza dei lavoratori (ai sensi dei commi 1 e 2) che in materia di protezione dei dati. Tanto, non solo con riguardo alla necessità di fornire agli interessati ogni necessaria informazione per assicurare ai dipendenti piena consapevolezza degli ulteriori trattamenti che il datore di lavoro si riserva di effettuare (circostanza che non ricorre nel caso di specie), ma anche mediante l’opportuna configurazione del sistema in modo che siano raccolti solo i dati necessari, nell’ambito dei limiti temporali individuati in relazione alla finalità principale per la quale il sistema è stato adottato (sul punto, v. Provv. 13 maggio 2021, n. 190, doc. web n. [9669974](#), par. 3.3.; v. già provv. 24 maggio 2017, n. 247, doc. web n. [6495708](#), spec. punto 5.3 e lett. e) dispositivo).

3.5 La sicurezza del trattamento.

In base al Regolamento, i dati devono essere “trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali” (art. 5, par. 1, lett. f), del Regolamento).

Al riguardo, l’art. 32 del Regolamento stabilisce che “tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio” e che “nel valutare l’adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare [...] dalla divulgazione non autorizzata [...] di] dati personali trasmessi, conservati o comunque trattati”.

In relazione al sistema di registrazione delle telefonate inbound “Phones”, realizzato dalla società IFM Infomaster S.p.A, attestato sui sistemi aziendali, si osserva che, alcune delle misure tecniche adottate non appaiono adeguate a proteggere i dati personali ivi contenuti. In primo luogo, è stato accertato che la password impostata dall’amministratore, all’atto della creazione di un nuovo utente, non doveva essere obbligatoriamente modificata al momento del primo accesso da parte dell’utente stesso (cfr. p. 7 del verbale del XX). In tal modo, si determina il venir meno, potenzialmente, del carattere riservato delle credenziali di accesso ai dati personali da parte dei soggetti autorizzati, non solo nei confronti dell’amministratore di sistema ma anche nei confronti degli altri utenti. Peraltro i rischi risulterebbero amplificati laddove il nome utente e la password scelta dall’amministratore siano impostati secondo un formato standard, noto a livello aziendale e quindi facilmente replicabile da altri utenti (es: nome utente pari a nome.cognome e prima password uguale al cognome).

Con riguardo alla tracciatura degli accessi alle telefonate registrate, le registrazioni – log file – delle operazioni effettuate non appaiono sufficienti, non essendo stata prevista la registrazione né dell’operato dei tecnici della società IFM sul sistema né delle operazioni di creazione e cancellazione delle utenze o di cancellazione di una registrazione (cfr. p. 9 del verbale del XX). Tali mancate registrazioni non consentono pertanto al titolare del trattamento di avere contezza, con certezza e in modo esaustivo, di tutti gli accessi alle telefonate registrate né lo rendono in

grado di documentare tali accessi.

Tale obbligo in capo al titolare, già presente nel previgente quadro normativo (ai sensi del disciplinare tecnico di cui all'allegato B al Codice, nel testo anteriore alle modifiche di cui al d.lgs. n. 101/2018), deriva, contrariamente a quanto sostenuto dalla Società nelle memorie difensive, dall'obbligo di adottare misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato anche rispetto al rischio di divulgazione non autorizzata o accesso illecito ai dati (art. 32 del Regolamento) e dal correlato obbligo di comprovarne l'adeguatezza (artt. 5, par. 2, e 24 Regolamento). In ragione della "responsabilità generale" del titolare del trattamento (art. 5, par. 2 del Regolamento) lo stesso è, infatti, tenuto a "mettere in atto misure adeguate ed efficaci [e...] dimostrare la conformità delle attività di trattamento con il [...] Regolamento, compresa l'efficacia delle misure" (cfr. considerando 74 nonché artt. 24 e 25 del Regolamento), fornendo a tal fine le necessarie indicazioni al fornitore del servizio (art. 28 del Regolamento).

Per tali ragioni, la Società si è resa responsabile della mancata adozione di misure tecniche e organizzative adeguate a garantire la riservatezza e l'integrità dei dati personali trattati mediante il sistema "Phones, in violazione degli artt. 5, par.1, lett. f) nonché 32 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento negli scritti difensivi della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice seppure meritevoli di considerazione e indicative della piena collaborazione del titolare del trattamento al fine di attenuare i rischi del trattamento, rispetto alla situazione presente all'atto dell'avvio dell'istruttoria, non consentono tuttavia di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano quindi insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Dalle verifiche compiute sulla base degli elementi acquisiti, anche attraverso la documentazione inviata dal titolare del trattamento, nonché dalle successive valutazioni, è stata accertata la non conformità di taluni trattamenti aventi ad oggetto dati personali dei dipendenti, mediante il sistema "Phones" attivato, in via definitiva, dal XX.

Per la determinazione della norma applicabile, sotto il profilo temporale, deve essere richiamato, in particolare, il principio di legalità di cui all'art. 1, comma 2, della l. n. 689/1981, ai sensi del quale le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati. Ciò determina l'obbligo di prendere in considerazione le disposizioni vigenti al momento della commessa violazione, che nel caso in esame – data la natura permanente degli illeciti contestati – deve essere individuato nell'atto di cessazione della condotta illecita. Nel prendere atto che il titolare del trattamento ha, nel corso dell'istruttoria, provveduto a conformare il trattamento ai principi del Regolamento, ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio presentato dal trattamento, si ritiene che, stante la cessazione dei trattamenti illeciti avvenuta successivamente nel maggio 2021, il Regolamento e il Codice costituiscano la normativa alla luce della quale valutare i trattamenti in questione.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dalla Società in quanto, fino alla disattivazione del sistema (XX) avvenuto in modo non conforme ai principi generali del trattamento nonché in violazione degli artt. 5, par. 1, lett. a), b), c) ed e), 6, 13, 25, 32 e 88, par. 2 del Regolamento e dell'art. 114 del Codice.

La violazione delle predette disposizioni rende inoltre applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83, parr. 4 e 5, del Regolamento.

In tale quadro, considerando che la condotta ha esaurito i suoi effetti (cfr. verbale audizione del XX, ove si legge che “allo stato il sistema di registrazione delle chiamate oggetto della presente istruttoria non è funzionante e tutti i dati e i metadati raccolti e memorizzati, ivi comprese le telefonate per le quali è stato effettuato il riascolto, sono stati cancellati e il trattamento è stato interrotto”), non ricorrono invece i presupposti per l'adozione di misure correttive, di cui all'art. 58, par. 2, del Regolamento.

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di “infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso” e, in tale quadro, “il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice” (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Ai fini dell'applicazione della sanzione è stato considerato che, sebbene la Società abbia dichiarato che i dipendenti addetti al call center fossero circa 20, la circostanza in base alla quale “oltre al personale in modalità stabile alla funzione di operatore di call center, vengono assegnati anche altri dipendenti temporaneamente non idonei alle mansioni per i quali sono stati assunti (ad esempio, autisti)” non consente di determinare con certezza il numero dei dipendenti complessivamente coinvolti dal trattamento, dovendosi, pertanto, presupporre che, seppur saltuariamente, le violazioni abbiano interessato un numero maggiore di interessati. Sono state altresì considerati: sia la specifica natura del trattamento – avviato in modo non conforme alla disciplina di settore in materia di impiego di strumenti tecnologici sul luogo di lavoro e alle indicazioni fornite nel tempo dal Garante, per i profili di competenza -, sia la prolungata durata del trattamento - che si è protratto dal XX al XX, termine della definitiva cessazione dello stesso.

Di contro, è stato considerato che il titolare del trattamento ha comunque prestato la propria collaborazione nel corso dell'istruttoria, provvedendo ad adottare, già a seguito dell'attività ispettiva condotta dall'Ufficio, taluni primi correttivi ai trattamenti oggetto di reclamo e ad avviare, in pari tempo, i necessari approfondimenti per assicurare la piena conformità dei trattamenti alle disposizioni in materia di protezione dei dati dei dipendenti, nel rispetto del principio di responsabilizzazione. Ai fini della commisurazione della complessiva sanzione è stato considerato altresì che il titolare del trattamento, le cui scelte sul piano tecnico e organizzativo sono state effettuate sulla base delle valutazioni espresse, anche in via informale, da propri consulenti e dal Responsabile della protezione dei dati, avesse confidato nella liceità dei trattamenti posti in essere.

Non risultano, inoltre, precedenti violazioni commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria, nella misura di euro 30.000,00 (trentamila) per la violazione degli artt. 5, 6, 13, 25, 32 e 88 del Regolamento, nonché 114 del Codice.

Tenuto conto degli specifici rischi per i diritti degli interessati derivanti dall'impiego di sistemi che comportano anche il controllo a distanza dei lavoratori, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e dall'art. 16 del Regolamento del Garante n. 1/2019.

Si ritiene, infine, che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO, IL GARANTE

rileva l'illiceità del trattamento effettuato da TPER Trasporto Passeggeri Emilia Romagna S.p.A. per la violazione degli artt. 5, 6, 13, 25, 32 e 88 del Regolamento e 114 del Codice, nei termini di cui in motivazione;

ORDINA

a TPER Trasporto Passeggeri Emilia Romagna S.p.A. in persona del legale rappresentante pro-tempore, con sede legale in Bologna, Via Saliceto n. 3, P.I. 03182161202, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 30.000,00 (trentamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di trenta giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

a TPER Trasporto Passeggeri Emilia Romagna S.p.A. di pagare la somma di euro 30.000,00 (trentamila) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice;

l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 28 ottobre 2021

IL PRESIDENTE
Stranzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei