Ordinanza ingiunzione nei confronti di Comune di Ginosa - 21 luglio 2022 [9811732]

[doc. web n. 9811732]

Ordinanza ingiunzione nei confronti di Comune di Ginosa - 21 luglio 2022

Registro dei provvedimenti
n. 270 del 21 luglio 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, 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 l'avv. Guido Scorza;

PREMESSO

1. Premessa.

Nell'ambito di un ciclo di attività ispettive, avente a oggetto le principali funzionalità di alcuni tra gli applicativi per l'acquisizione e gestione delle segnalazioni di illeciti più diffusamente impiegati dai datori di lavoro pubblici e privati nel quadro della disciplina in materia di segnalazione di condotte

illecite (c.d. whistleblowing), che prevede specifiche garanzie a tutela dell'identità del segnalante, sono stati effettuati - anche alla luce di quanto disposto, con riguardo all'attività ispettiva di iniziativa curata dall'Ufficio del Garante, con deliberazioni del 12 settembre 2019, doc. web n. 9147297, del 6 febbraio 2020, doc. web n. 9269607, e del 1° ottobre 2020, doc. web n. 9468750 - specifici accertamenti nei confronti di Clio S.r.l. (di seguito "Clio" o "Fornitore"), che fornisce e gestisce per conto di diversi soggetti, pubblici e privati, l'applicativo utilizzato per l'acquisizione e la gestione delle segnalazioni di condotte illecite (v. verbali delle operazioni compiute del XX).

Nel corso dell'attività ispettiva è stato accertato che il predetto applicativo è utilizzato anche dal Comune di Ginosa (di seguito "Comune").

2. L'attività istruttoria.

Nel corso dell'attività ispettiva presso il Fornitore, è emerso quanto segue:

Clio ha fornito un elenco dei clienti, tra cui il Comune, a cui "offre il servizio per l'acquisizione e la gestione delle segnalazioni di condotte illecite" e ha rappresentato che "[…] non si avvale di sub-responsabili per l'esecuzione di attività di trattamento" (v. verbale del XX, p. 3, e all. 3);

Clio è stata designata quale responsabile del trattamento unicamente da alcuni clienti, mentre altri, tra cui il Comune, "non hanno provveduto a individuare la Società come responsabile del trattamento ai sensi dell'art. 28 del Regolamento" (v. verbale del XX, p. 3 e all. 4, 5 e 6);

> "l'applicativo whistleblowing, raggiungibile da rete pubblica a un indirizzo web del tipo "https://nomeente.whistleblowing.name", viene messo a disposizione dei clienti in modalità Software as a Service (SaaS). Tale modalità di erogazione del servizio, a parere della Società, rappresenta una specifica garanzia a tutela dell'identità dei segnalanti in quanto consente la gestione dei dati presso un soggetto diverso dall'amministrazione datore di lavoro. L'applicativo in questione, sviluppato da Clio, è installato su server presso il data center della Società ed è configurato in modalità multitenant. L'applicativo consente unicamente l'acquisizione delle segnalazioni da parte dei dipendenti e non consente l'acquisizione di segnalazioni anonime o da parte di soggetti esterni alle amministrazioni. Poiché alcuni clienti hanno rappresentato la necessità di acquisire anche segnalazioni anonime o da parte di soggetti esterni, la Società sta sviluppando una nuova versione dell'applicativo che consentirà anche l'acquisizione di tali tipologie di segnalazioni e che sarà messa in produzione nel corso dell'anno 2020. La Società fornisce servizi di assistenza e manutenzione" (v. verbale del XX, p. 4);
>
> "in fase di attivazione del servizio per un nuovo ente, [Clio] provvede […] a creare la chiave utilizzata per cifrare i dati relativi alle segnalazioni memorizzati all'interno del database dell'applicativo in ambiente di produzione" (v. verbale del XX, p. 5).

Successivamente, con nota del XX, il Fornitore, a integrazione della documentazione e delle informazioni fornite nel corso dell'attività ispettiva, ha comunicato di aver "inviato ai […] Clienti che non l'hanno ancora fatto, sollecito via pec per il conferimento della nomina di Clio a Responsabile in outsourcing del trattamento dei dati, comunicando che, in difetto di riscontro entro sette giorni lavorativi avremmo sospeso il servizio sino alla regolarizzazione" (p. 1).

Da ultimo, in riscontro a una specifica richiesta d'informazioni da parte dell'Ufficio, il Fornitore, in data XX, ha ulteriormente precisato che il rapporto con il Comune– per il quale, all'epoca delle attività ispettive, era stata acquisita mediante l'applicativo in questione, almeno una reale segnalazione di condotte illecite non riconducibile, quindi, a mere attività di prova o di verifica del funzionamento dell'applicativo – è stato disciplinato ai sensi dell'art. 28 del Regolamento "a seguito delle pec di sollecito" inviate dal Fornitore.

Con nota del XX, l'Ufficio, sulla base degli elementi acquisiti, ha notificato al Comune, 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 il Comune ha posto in essere trattamenti di dati personali di dipendenti e altri interessati, mediante l'utilizzo dell'applicativo per l'acquisizione e gestione delle segnalazioni illecite, non avendo regolamentato il rapporto con il Fornitore, in violazione dell'art. 28 del Regolamento; mettendo a disposizione dello stesso Fornitore dati relativi alle segnalazioni di illeciti in assenza di un'idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a), e 6 del Regolamento e dell'art. 2-ter del Codice.

Con nota del XX, il Comune ha fatto pervenire le proprie memorie precisando, tra l'altro, che:

> "dall'analisi documentale a supporto della mappatura dei trattamenti all'interno dei singoli servizi/settori dell'Ente locale, il contratto di servizi sottoscritto con la società CLIO, avveniva con Determinazione nr. 28 /EC del 23 febbraio 2015 […] e dunque, risalente ad un periodo temporale antecedente all'entrata in vigore del Regolamento Europeo";
>
> "il contratto prevedeva clausole specifiche di riservatezza secondo le quali erano desumibili i ruoli svolti dai soggetti reciprocamente obbligati (il Comune quale Titolare del trattamento e la società CLIO affidataria del servizio quale responsabile), comprensivi della ripartizione in ordine alle responsabilità reciproche in tema di privacy e Data Protection, in relazione alla gestione delle segnalazioni (Whistleblowing)";
>
> "successivamente, il Comune di Ginosa, provvedeva al rinnovo del servizio di affidamento per la gestione delle segnalazioni alla Società Clio, in ossequio a quanto previsto dall'art. 6 comma 1 lettera c del Reg. UE e tenuto conto delle prescrizioni previste anche dall'art 32 REG.UE relativo alle misure tecniche idonee a garantire le specificità del servizio […], ispirate al provv. 4 dicembre 2019, doc. web n. 9215763, con il quale ha reso il parere ad ANAC sullo schema di "Linee guida in materia […]";
>
> "ciò posto, la predisposizione dell'addendum contrattuale previsto dall'Art. 28 GDPR avveniva nel mese di novembre 2019, in seguito all'attività di mappatura dei trattamenti in essere presso l'ente. Il suddetto addendum contrattuale veniva poi inoltrato e sottoscritto in data XX […]. Nelle more della sottoscrizione della suddetta nomina non risulta al sottoscritto Comune che vi siano state delle segnalazioni pervenute sul portale";
>
> "per quanto attiene alla presunta segnalazione avvenuta in assenza della regolare formalizzazione della Nomina a Resp. esterno del trattamento si precisa quanto segue: Risulta agli atti del sottoscritto Ente che la segnalazione citata sia relativa al mese di marzo 2018 […] e, pertanto, attiene ad un periodo anteriore rispetto alla cogenza del Regolamento e all'obbligatorietà dell'addendum come prescritto dall'art. 28 GDPR. Tra l'altro, si sottolinea che, la segnalazione effettuata, inoltrata anche all'Anac, non avendo avuto alcun seguito, né irrogazione di sanzione alcuna, ha comportato un'archiviazione da parte dell'Ente";
>
> "non risulta agli atti del sottoscritto Ente che vi siano state altre segnalazioni a mezzo dell'applicativo nel periodo tra marzo 2018 e agosto 2021, pertanto alcun trattamento può essere riconosciuto in capo all'applicativo e quindi alla società";
>
> "benché l'addendum contrattuale ex art. 28 non sia stato predisposto nell'imminenza della piena applicazione del Reg. UE, ma sia stata predisposta (ritardata) solo nel mese di novembre del 2019 […] di fatto, nelle more, non vi è stato alcun trattamento di dati

sull'applicativo acquisito per la gestione delle segnalazioni che possa aver compromesso la liceità del medesimo".
In data XX si è, inoltre, svolta l'audizione richiesta dal Comune, ai sensi dell'art. 166, comma 6, del Codice, in occasione della quale lo stesso ha confermato quanto già dichiarato in sede di memorie difensive, precisando, tra l'altro, che:

"la nomina a responsabile della società fornitrice del servizio per l'acquisizione e la gestione delle segnalazioni di condotte illecite è stata effettuata dal Comune nel mese di novembre 2019, a seguito di un progressivo adeguamento alla normativa in materia di protezione dei dati che ha richiesto dei passaggi obbligati, anche in ragione delle difficoltà che gli enti locali di piccole dimensioni hanno incontrato nell'adeguarsi alle disposizioni delle normative di settore, che impongono specifici obblighi a carico degli stessi. Ciò, non solo riguardo alla disciplina in materia di protezione dei dati, ma anche con riguardo alle altre norme di settore come quella sulla trasparenza amministrativa";

"il contratto con la società, in essere dal 2015 e automaticamente rinnovato nel corso del tempo, conteneva già alcuni elementi che il Comune riteneva sufficienti per regolare il rapporto con il fornitore anche sotto il profilo della protezione dei dati";

"la segnalazione presente all'interno dell'applicativo whistleblowing al momento dell'accertamento ispettivo dell'Autorità è stata ricevuta dal Comune in un momento antecedente alla data in cui il Regolamento (UE) 2016/679 è divenuto pienamente applicabile";

"la segnalazione è stata trattata nel rispetto della disciplina di settore a tutela della riservatezza dell'identità del dipendente che segnala illeciti, trasmessa all'ANAC per i profili di competenza e successivamente archiviata".

3. Esito dell'attività istruttoria. La normativa applicabile: la disciplina in materia di tutela del dipendente che segnala illeciti e la disciplina in materia di protezione dei dati personali.

L'adozione di sistemi di segnalazione di illeciti (c.d. whistleblowing), per le proprie implicazioni in materia di protezione dei dati personali, è da tempo all'attenzione delle Autorità di controllo (Segnalazione del Garante al Parlamento e al Governo reperibile in www.garanteprivacy.it, doc. web n. 1693019; v., anche, Gruppo di Lavoro Art. 29, "Parere 1/2006 relativo all'applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria", adottato il 1° febbraio 2006, doc. web n. 1607645).

Numerosi sono stati, in questi anni, gli interventi da parte del Garante, anche di carattere generale, in materia (cfr., da ultimo, provv.ti 7 aprile 2022, nn. 134 e 135, doc. web nn. 9768363 e 9768387, e precedenti in essi richiamati; v. anche provv. 4 dicembre 2019, n. 215, doc. web n. 9215763, parere del Garante sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)" di ANAC).

Nel corso di un'audizione in Parlamento, il Garante ha ricordato che nell'esercizio della delega per il recepimento della Direttiva (UE) 2019/1937 (riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione) è necessario "realizzare un congruo bilanciamento tra l'esigenza di riservatezza della segnalazione- funzionale alla tutela del segnalante -, la necessità di accertamento degli illeciti e il diritto di difesa e al contraddittorio del segnalato. La protezione dei dati personali è, naturalmente, un fattore determinante per l'equilibrio tra queste istanze e per ciò è opportuno un coinvolgimento del Garante in fase di esercizio della delega" (cfr., Audizione del

Garante per la protezione dei dati personali sul d.d.l. di delegazione europea 2021, Senato della Repubblica-14esima Commissione parlamentare dell'Unione europea, 8 marzo 2022, doc. web n. 9751458).

A livello nazionale, la materia è stata disciplinata, in un primo momento, nel quadro delle norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche (cfr. art. 54-bis del d.lgs. 30 marzo 2001, n. 165, introdotto dall'art. 1, comma 51, della l. n. 190/2012, recante disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione). Successivamente il quadro normativo è stato definito con la l. 30 novembre 2017, n. 179 (in G.U. 14 dicembre 2017, n. 291) recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" che ha modificato la disciplina relativa alla "tutela del dipendente pubblico che segnala illeciti" (cfr. nuova versione dell'art. 54-bis del d.lgs. n. 165/2001 e art. 1, comma 2, della l. n. 179/2017) ed ha introdotto una nuova disciplina in materia di whistleblowing riferita ai soggetti privati, integrando la normativa in materia di "responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (cfr. art. 2 della l. n. 179/2017 che ha aggiunto il comma 2-bis all'art. 6 del d.lgs. 8 giugno 2001, n. 231).

In tale quadro, i soggetti obbligati al rispetto delle richiamate disposizioni devono trattare i dati necessari all'acquisizione e gestione delle segnalazioni nel rispetto anche della disciplina di protezione dei dati personali (spec. artt. 6, par. 1, lett. c), 9, par. 2, lett. b), 10 e 88, par. 1, del Regolamento; sul punto, v., da ultimo, provv.ti 7 aprile 2022, nn. 134 e 135, doc. web nn. 9768363 e 9768387, 10 giugno 2021, nn. 235 e 236, doc. web nn. 9685922 e 9685947).

Per tali ragioni, la disciplina di settore sopra richiamata, che comporta trattamenti dei dati del dipendente che segnala illeciti, deve essere considerata come una delle "norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" previste dall'art. 88, par. 1, del Regolamento (cfr., da ultimo, provv.ti 10 giugno 2021, nn. 235 e 236, doc. web nn. 9685922 e 9685947; cfr. newsletter n. 480 del 2 agosto 2021, doc. web n. 9687860; ma v. già provv. 4 dicembre 2019, n. 215, doc. web n. 9215763, parere del Garante sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)" di ANAC).

In generale, sebbene sul titolare del trattamento, che determina le finalità e le modalità del trattamento dei dati, ricada una "responsabilità generale" per i trattamenti posti in essere (v. art. 5, par. 2, c.d. "accountability", e 24 del Regolamento), anche quando questi siano effettuati da altri soggetti "per suo conto" (cons. 81, artt. 4, punto 8), e 28 del Regolamento), il Regolamento ha disciplinato gli obblighi e le altre forme di cooperazione cui è tenuto il responsabile del trattamento e l'ambito delle relative responsabilità (v. artt. 30, 32, 33, par. 2, 82 e 83 del Regolamento; cfr., tra i tanti, provv. 10 febbraio 2022, n. 43, doc. web n. 9751498 e i precedenti provv. ivi richiamati).

Il responsabile del trattamento è legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare" (art. 28, par. 3, lett. a), del Regolamento) e il rapporto tra titolare e responsabile è regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, consente al titolare di impartire istruzioni al responsabile anche sotto il profilo della sicurezza dei dati e prevede, in dettaglio, quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare e del responsabile. Inoltre, il responsabile del trattamento deve assistere il titolare nel garantire il rispetto degli obblighi derivanti dalla disciplina di protezione dati, "tenendo conto della natura del trattamento" e dello specifico regime applicabile allo stesso (art. 28, par. 3, lett. f), del Regolamento).

Più in generale, il titolare del trattamento è comunque tenuto a rispettare i principi in materia di

protezione dei dati (art. 5 del Regolamento) e 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” (artt. 5, par. 1, lett. f), del Regolamento).

Il titolare, nell’ambito della necessaria individuazione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame (artt. 24, 25 e 32 del Regolamento), deve definire il proprio modello di gestione delle segnalazioni in conformità ai principi della “protezione dei dati fin dalla progettazione” e della “protezione per impostazione predefinita”, tenuto conto anche delle osservazioni presentate al riguardo dal responsabile della protezione dei dati (RPD).

3.1 Mancata regolamentazione del rapporto con il Fornitore.

Il titolare, nell’ambito della predisposizione delle misure tecniche e organizzative che soddisfino i requisiti stabiliti dal Regolamento, anche sotto il profilo della sicurezza (artt. 24 e 32 del Regolamento), può avvalersi di un responsabile per lo svolgimento di alcune attività di trattamento, cui impartisce specifiche istruzioni (cfr. considerando 81 del Regolamento). In tal caso il titolare “ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto [le predette misure] adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti degli interessati” (art. 28, par. 1, del Regolamento. Sul punto si osserva che il titolare del trattamento è tenuto a “mettere in atto misure adeguate ed efficaci [e a …] dimostrare la conformità delle attività di trattamento con il […] Regolamento, compresa l’efficacia delle misure” adottate (cons. 74 del Regolamento).

Ai sensi dell’art. 28 del Regolamento, il titolare può quindi affidare un trattamento anche a soggetti esterni, disciplinandone il rapporto con un contratto o un altro atto giuridico e impartendo le istruzioni in merito ai principali aspetti del trattamento, in particolare, per i profili di interesse nel presente procedimento: “la durata del trattamento”, “gli obblighi e i diritti del titolare del trattamento”, nonché le operazioni da effettuare “dopo che è terminata la prestazione dei servizi relativi al trattamento” (art. 28, par. 3, del Regolamento).

Il responsabile del trattamento è, pertanto, legittimato a trattare i dati degli interessati “soltanto su istruzione documentata del titolare” (art. 28, par. 3, lett. a), del Regolamento; al riguardo v. Cass., Sez. I Civ., ordinanza n. 21234 del 23 luglio 2021).

Nel caso di specie, il Comune, titolare del trattamento, tenuto all’osservanza degli obblighi derivanti dalla disciplina di settore, anziché realizzare in autonomia un applicativo per l’acquisizione e gestione delle segnalazioni di illeciti, ha assunto la decisione di avvalersi dei servizi offerti da una società esterna, fornitrice dell’applicativo. Pertanto, il Fornitore dell’applicativo whistleblowing ha trattato i dati personali dei segnalanti e degli altri interessati indicati nelle segnalazioni (soggetti segnalati, testimoni, ecc.), nell’ambito di un servizio strumentale, finalizzato all’acquisizione e alla gestione di segnalazioni di illeciti, per conto e nell’interesse del Comune, nell’adempimento di obblighi di legge gravanti su quest’ultimo.

Le funzioni svolte dal Fornitore hanno quindi comportato un trattamento dei dati personali dei segnalanti e degli altri interessati indicati nelle segnalazioni (soggetti segnalati, testimoni, ecc.) di cui il Comune risulta comunque titolare, trattandoli in base ad un preciso obbligo di legge e determinando i mezzi e le modalità del trattamento, nonché i principali termini dell’esecuzione del servizio sulla base di specifici contratti.

In tali casi la disciplina in materia di protezione dei dati richiede che il rapporto tra il titolare e il fornitore sia regolato da un contratto o da altro atto giuridico a sensi dell’art. 28 del Regolamento (v. anche considerando 81 e art. 4, punto 8, del Regolamento), anche al fine di evitare trattamenti

(comunicazione a terzi) in assenza di idoneo presupposto di liceità (stante la nozione di “terzo” di cui all’art. 4, punto 10, del Regolamento; cfr. art. 2-ter, commi 1 e 4, lett. a), del Codice, con riguardo alla definizione di “comunicazione”). Ciononostante, con riguardo al caso di specie, il rapporto tra il Comune e il Fornitore non è stato opportunamente regolato sotto il profilo della protezione dei dati, come risulta dalla documentazione in atti.

Sebbene nella memoria difensiva il titolare abbia dichiarato che il contratto sottoscritto nel 2015 con il Fornitore “prevedeva clausole specifiche di riservatezza secondo le quali erano desumibili i ruoli svolti dai soggetti reciprocamente obbligati (il Comune quale Titolare del trattamento e la società CLIO affidataria del servizio quale responsabile), comprensivi della ripartizione in ordine alle responsabilità reciproche in tema di privacy e Data Protection, in relazione alla gestione delle segnalazioni (Whistleblowing)”, si rileva che invece il contratto di fornitura del servizio (cfr. all. 1 e 2 alla nota del XX) non aveva le specifiche caratteristiche dell’atto giuridico che definisce il ruolo del responsabile, in quanto non contiene gli elementi previsti dall’art. 28 del Regolamento (cfr. spec. par. 3).

Il Comune ha altresì dichiarato che l’unica “segnalazione [ricevuta] in assenza della regolare formalizzazione della Nomina a Resp[onsabile] esterno del trattamento [fosse] relativa al mese di marzo 2018 [...] e, pertanto, attiene ad un periodo anteriore rispetto alla cogenza del Regolamento e all’obbligatorietà dell’addendum come prescritto dall’art. 28 GDPR”.

Al riguardo occorre precisare che, sebbene il trattamento sia stato avviato dal Comune nel periodo precedente all’entrata in vigore del Regolamento (essendo il sistema adottato fin dal 2015 e la segnalazione acquisita tramite il sistema nel marzo del 2018), ai fini della individuazione della normativa applicabile, sotto il profilo temporale, occorre tener presente che, in base al principio di legalità di cui all’art. 1, comma 2, della l. n. 689/1981, “Le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati”. Da ciò consegue la necessità di prendere in considerazione le disposizioni vigenti al momento della commessa violazione; nel caso in esame, data la natura permanente dell’illecito contestato, tale momento deve essere individuato all’atto della cessazione della condotta illecita, avvenuta nel mese di novembre 2019 con la regolamentazione del rapporto con il Fornitore ai sensi dell’art. 28 del Regolamento e, quindi, nella piena vigenza delle disposizioni del Regolamento e del Codice (come modificato dal d.lgs. 101/2018). Per le medesime ragioni non può ritenersi rilevante neanche la circostanza per la quale l’unica segnalazione acquisita tramite il predetto applicativo fosse risalente al marzo del 2018, tenuto conto che la stessa risultava ancora presente sul sistema all’epoca degli accertamenti del Garante.

D’altronde l’obbligo di regolamentare il rapporto con soggetti che agiscono per conto e nell’interesse del titolare era già previsto dal quado previgente , (v., artt. 4, lett. g) e 29 del Codice, anteriormente alle modifiche di cui al d.lgs. n.101/2018, che prevedeva "I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento (comma 4-bis)....Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4 bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4 bis. (comma 5)"; al riguardo, Cass., Sez. I Civ., ordinanza n. 21234 del 23 luglio 2021).

La violazione delle predette diposizioni, ancorché non comportasse l’applicazione di una sanzione amministrativa (diversamente da quanto ora previsto dagli artt. 28 e 83, par. 4, del Regolamento) dava comunque luogo a trattamenti non conformi alla disciplina di protezione di dati potendosi configurare una comunicazione illecita di dati personali in favore di un soggetto che, non essendo stata designato come responsabile, era terzo rispetto al trattamento (sul punto, v. anche successivo par. 4.2).

Risulta pertanto accertato che – ferme restando le valutazioni in ordine alla liceità del trattamento svolto dal Fornitore, oggetto di autonomo procedimento – il Comune, fino al mese di novembre 2019, ha operato in violazione dell'art. 28 del Regolamento non avendo disciplinato sotto il profilo della protezione dei dati il rapporto con il Fornitore.

3.2 Illecito trattamento dei dati relativi alle segnalazioni whistleblowing.

Alla luce delle considerazioni che precedono e della documentazione in atti, nel periodo che va dal marzo 2018 al novembre 2019, stante l'assenza di una regolamentazione del rapporto con il Fornitore ai sensi dell'art. 28 del Regolamento, il Comune, avvalendosi dei servizi da questi offerti, al fine di dotare la propria struttura di un efficacie e efficiente sistema di acquisizione e gestione di segnalazioni di condotte illecite, come prescritto dalla legge, ha messo a diposizione del Fornitore dati personali relativi a segnalazioni di condotte illecite, consentendogli di raccoglierle e conservarle mediante l'applicativo whistleblowing, in assenza di idoneo presupposto normativo.

Né rileva la circostanza che, successivamente alla sua acquisizione, la segnalazione di condotte illecite, presente nell'applicativo whistleblowing all'epoca delle attività ispettive dell'Autorità, sia stata archiviata, atteso che anche la sola raccolta e conservazione di dati personali configura un trattamento soggetto alla disciplina in materia di protezione dei dati (v. art. 4, punto 2), del Regolamento).
Considerata la mancata regolamentazione del rapporto con il Fornitore sotto il profilo della protezione dei dati, si ritiene che, come già in precedenza chiarito dal Garante con riguardo ad analoghe fattispecie (cfr. provv. del 7 marzo 2019, n. 81, doc. web n. 9121890; provv. 17 settembre 2020, n. 160, doc. web n. 9461168; provv. 17 dicembre 2020, n. 280, doc. web n. 9524175; v. anche le "Linee guida 07/2020 sui concetti di titolare e responsabile del trattamento nel GDPR", adottate il 7 luglio 2021 dal Comitato europeo per la protezione dei dati personali, spec. nota 42), il Comune abbia messo a disposizione del Fornitore i dati personali relativi alle segnalazioni di illeciti acquisiti mediante l'applicativo whistleblowing, in assenza di un'idonea base giuridica, dando luogo a un trattamento illecito di dati personali, in violazione degli artt. 5, par. 1, lett. a), e 6 del Regolamento e dell'art. 2-ter del Codice.

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.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato in quanto avvenuto in violazione degli artt. 5, par. 1, lett. a), 6 e 28 del Regolamento e dell'art. 2-ter del Codice.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83, parr. 4 e 5, del Regolamento e dell'art. 166, comma 2, del Codice.

In tale quadro, considerando che la condotta ha esaurito i suoi effetti, 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 – considerando anche il richiamo contenuto nell'art. 166, comma 2, del Codice – 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 sono stati considerati la natura, l'oggetto e la finalità del trattamento la cui disciplina di settore prevede, a tutela dell'interessato, un elevato grado di riservatezza con specifico riguardo all'identità dello stesso.

Di contro, è stato considerato che il Comune è un ente di piccole dimensioni, con risorse finanziarie limitate, e che al momento delle attività ispettive era presente una sola segnalazione di condotte illecite all'interno dell'applicativo in questione. Inoltre, il Comune ha collaborato nel corso dell'istruttoria provvedendo ad adottare, già a seguito dell'attività ispettiva condotta dall'Ufficio, misure tecniche e organizzative volte a conformare i trattamenti in corso alla disciplina in materia di protezione dei dati personali, nel rispetto del principio di responsabilizzazione, disciplinando il rapporto con il Fornitore ai sensi dell'art. 28 del Regolamento. 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 5.000,00 (cinquemila) per la violazione degli artt. 5, par. 1, lett. a), 6 e 28 del Regolamento e dell'art. 2-ter del Codice.

Tenuto conto della particolare natura dei dati personali oggetto di trattamento e dei connessi rischi per il segnalante e gli altri interessati nel contesto lavorativo, 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 ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO, IL GARANTE

rileva l'illiceità del trattamento effettuato dal Comune di Ginosa. per la violazione degli artt. 5, par. 1, lett. a), 6 e 28 del Regolamento e dell'art. 2-ter del Codice, nei termini di cui in motivazione;

ORDINA

al Comune di Ginosa, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Marconi, 74013 Ginosa (TA), C.F. 80007530738, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 5.000,00 (cinquemila) 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

al Comune di Ginosa di pagare la somma di euro 5.000,00 (cinquemila) 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, 21 luglio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei