Ordinanza ingiunzione nei confronti di Clio s.r.l. - 21 luglio 2022 [9811271]

[doc. web n. 9811271]

Ordinanza ingiunzione nei confronti di Clio s.r.l. - 21 luglio 2022

Registro dei provvedimenti
n. 268 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 specifici accertamenti nei confronti di Clio S.r.l. (di seguito "Clio" o "Società"), 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).

Ciò 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.

2. L'attività istruttoria.

Nel corso dell'attività ispettiva presso la Società, è emerso quanto segue:

la Società "ha fornito copia del registro delle attività di trattamento svolte dalla Società in qualità di titolare del trattamento […], rappresentando che lo stesso è tenuto […] in formato elettronico", all'interno del quale "è censita l'attività di erogazione del servizio di whistleblowing rispetto alla quale la società si definisce "Responsabile dei clienti"" (v. verbale del XX, p. 3 e all. 1);

"la Società, allo stato, non ha ancora istituito il registro delle attività di trattamento svolte in qualità di responsabile per conto dei propri clienti" (v. verbale del XX, p. 3);

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

la Società è stata nominata responsabile del trattamento da alcuni clienti, mentre altri "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);

"l'accesso all'applicativo whistleblowing è consentito mediante credenziali di autenticazione composte da una username (di regola, un indirizzo e-mail) e da una password. Sono stati previsti cinque diversi profili di autorizzazione: (1) profilo "Amministratore dell'applicativo", in uso al personale della Società, che consente l'attivazione e la disattivazione delle diverse istanze dell'applicativo nonché la creazione dell'utente con il profilo "Responsabile"; (2) profilo "Responsabile", in uso al RPCT dell'ente, che consente la visualizzazione e la gestione delle segnalazioni; (3) profilo "Staff Anti-corruzione", in uso al personale di staff del

RPCT, che ha un ruolo di supporto nella gestione istruttoria delle segnalazioni senza possibilità di conoscere l'identità dei segnalanti; (4) profilo "Gestione utenti" che consente unicamente la gestione delle utenze in uso al personale dell'ente e non consente l'accesso ai dati delle segnalazioni; (5) profilo "Segnalante" che consente al personale dell'ente di effettuare una segnalazione e di verificare lo stato di lavorazione delle proprie segnalazioni" (v. verbale del XX, p. 4);

la Società ha evidenziando che "a ogni utenza può essere attribuito un solo profilo e che, ove fosse necessario, attribuire più profili al medesimo soggetto (ad esempio, in qualità di segnalante e di persona di staff del RPCT) è necessario creare distinte utenze, una per ciascun profilo" (v. verbale del XX, p. 2);

la Società ha rappresentato che "in fase di attivazione del servizio per un nuovo ente, 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);

la Società "ha rappresentato che, in caso di cessazione del contratto di fornitura del servizio, la Società rende disponibile al RPCT dell'ente un export cifrato dei dati delle segnalazioni acquisite prima della cancellazione degli stessi" (v. verbale del XX, p. 4).

Successivamente, con nota del XX, la Società, 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" e di aver "modificato le condizioni di utilizzo e subordinato il perfezionamento dell'acquisto MEPA all'acquisizione della nomina a Responsabili del trattamento ai sensi dell'art. 28 GDPR" (p. 1 e all. 4).

Da ultimo, in riscontro a una specifica richiesta di informazioni da parte dell'Ufficio, la Società, in data XX, ha ulteriormente precisato che i rapporti con i clienti – per i quali, 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) e per i quali era ancora in corso il contratto di fornitura dell'applicativo in questione (Comune di Ginosa e Acqua Novara.VCO S.p.a.) – sono stati disciplinati ai sensi dell'art. 28 del Regolamento "a seguito delle pec di sollecito" inviate dalla Società. Gli altri contratti sono stati invece conclusi con la risoluzione del contratto e la disattivazione del servizio.

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 – stante la mancata regolamentazione del rapporto con taluni clienti, titolari del trattamento, ai sensi dell'art. 28 del Regolamento – il trattamento di dati personali posto in essere dalla Società, fino alla regolamentazione del rapporto con i clienti, sia avvenuto 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, nonché in mancanza della tenuta del registro delle attività di trattamento svolte per conto dei titolari del trattamento, in violazione dell'art. 30, par. 2, del Regolamento.

Con nota del XX, la Società ha fatto pervenire le proprie memorie difensive, precisando, tra l'altro, che:

“la gran parte dei contratti per il servizio erogato attraverso l’applicativo “Whistleblowing” di CLIO sono stati attivati negli anni 2016/2017, subito dopo l’entrata in vigore della normativa sul Whistleblowing in Italia e le linee guida ANAC del 2015 e prima dell’entrata in vigore del Regolamento UE n. 679/2016, nella vigenza dell’art. 29 del D. Legislativo 196/2003 che configurava la nomina a Responsabile del trattamento da parte del titolare quale “facoltà” e non obbligo”;

“È probabilmente da attribuire a tale ragione il fatto che nei successivi rinnovi - avvenuti tramite contatti tra i rispettivi uffici amministrativi/contabili - non si sia provveduto all’adeguamento all’art. 28 del Regolamento con un’investitura “formale” di CLIO a Responsabile del trattamento a latere del Contratto di fornitura. Tuttavia quest’ultimo implicava de facto un tale ruolo da parte del fornitore che, come avete potuto constatare nel Registro dei Trattamenti aziendale, tale si qualificava. Anche ANAC nelle linee guida 2021 considera il fornitore del servizio logicamente Responsabile del trattamento”;

“gli Enti che avevano nominato CLIO quale responsabile avevano contrattualizzato il servizio per la prima volta nel corso dell’anno 2019 nel vigore del GDPR e, quindi, con delle procedure oramai standardizzate nella conclusione dei contratti che prevedevano di default l’acquisizione della nomina ex art. 28 del GDPR anche in ragione dell’istituzione della figura del DPO, la cui piena operatività ha richiesto del tempo rispetto alla data di entrata in vigore del Regolamento (25 maggio 2018)”;

“Negli altri casi, l’assenza della nomina a Responsabile, non ha comportato danni e/o trattamenti illegittimi da parte di CLIO o comunque contrari ai principi di liceità, trasparenza e correttezza. La società non ha mai trattato alcun dato per finalità diverse, non pertinenti o eccedenti le attività necessarie ad erogare il servizio contrattualizzato con i propri Clienti”;

“alcun dato relativo alle segnalazioni è stato divulgato o altrimenti reso accessibile all’esterno, né al personale interno all’azienda”, avendo limitato le proprie attività a talune operazioni, quali, in particolare, “la manutenzione sistemistica automatica per garantire il back-up del server” e “gli aggiornamenti applicativi nel caso di evoluzione normativa”;

“si contesta l’assunto per il quale l’assenza della nomina ex art. 28 GDPR comporti automaticamente per CLIO l’aver operato il trattamento di dati personali in violazione dell’art. 5 ed in assenza delle condizioni di liceità previste dell’art. 6 del Regolamento, né sul piano sostanziale ma neppure su quello formale. La nomina non rappresenta l’unica base legittima di un trattamento di dati, se gli stessi sono trattati in maniera conforme alle prescrizioni del Regolamento e delle altre leggi che regolano una specifica materia, com’è nel caso di specie la disciplina sul Whistleblowing che si fonda proprio sui presupposti della riservatezza e sicurezza dei dati […] Anche ANAC all’interno delle linee guida 2021 riporta testualmente alle pagg. 6-7 “…In questo ambito, i trattamenti di dati personali effettuati dai soggetti obbligati possono essere considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, § 1, lett. c) del Regolamento), e, con riguardo a categorie particolari di dati (art. 9, § 2, lett. b) del Regolamento in relazione all’art. 54-bis) o a dati relativi a condanne penali e reati, possono, altresì, essere considerati necessari per l’esecuzione di un compito di interesse pubblico contemplato dall’ordinamento (art. 6, § 1, lett. e) e art. 9, § 2, lett. g) e 10 del Regolamento)””.

“[dopo l’attività ispettiva del Garante] si sono succeduti copiosi interventi regolamentari, pareri, consultazioni, linee guida (ad esempio, il primo parere del Garante Privacy ad ANAC è del 4 dicembre 2019) sui temi della Privacy e del Whistleblowing che dimostrano come calare i principi normativi nella realtà operativa degli Enti e dei fornitori non è un processo semplice, ma richiede interventi chiarificatori e di supporto in ordine agli adempimenti ed alle procedure da adottare ai fini di dare corretta attuazione alle norme”;

“è stato regolarmente popolato il Registro dei trattamenti”;

“In seguito all’ispezione, [la Società] si è attivata per individuare le criticità e migliorare le procedure aziendali in un’ottica di corretta adesione al dettato normativo sia dal punto di vista formale che sostanziale”.

Sebbene la Società avesse espressamente richiesto di partecipare all’audizione presso l’Autorità, ai sensi dell’art. 166, comma 6, del Codice, si dà conto che la stessa ha successivamente rinunciato ad essere audita, richiamando, con una specifica nota, le considerazioni già espresse nei propri scritti difensivi (cfr. nota XX, in atti).

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 questo ambito, i trattamenti di dati personali effettuati dai soggetti, pubblici e privati, tenuti al rispetto del predetto quadro giuridico – che contiene "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 – possono essere considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (artt. 6, par. 1, lett. c), 9, par. 2, lett. b), e 10 del Regolamento).

In tale quadro il titolare del trattamento, 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), può comunque ricorrere a un responsabile del trattamento per lo svolgimento di alcune attività di trattamento, cui impartisce specifiche istruzioni (cons. 81, artt. 4, punto 8), e 28 del Regolamento) e 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" (art. 25 del Regolamento), tenuto conto anche delle osservazioni presentate al riguardo dal responsabile della protezione dei dati (RPD).

3.1. Liceità dei trattamenti effettuati dalla Società fornitrice dell'applicativo whistleblowing.

Ai fini del rispetto della normativa in materia di protezione dei dati personali occorre, in via preliminare, identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella di titolare e di responsabile del trattamento e dei soggetti che operano sotto la diretta responsabilità di questi (art. 4, punti 7 e 8, 28 e 29 del Regolamento).

Come chiarito in numerose occasioni dal Garante, i soggetti obbligati al rispetto delle richiamate disposizioni devono trattare i dati necessari all'acquisizione e gestione delle segnalazioni anche nel rispetto della disciplina in materia di protezione dei dati personali (v., sul punto, provv.ti 10 giugno 2021, nn. 235 e 236, doc. web nn. 9685922 e 9685947, 7 aprile 2022, nn. 134 e 135, doc. web nn. 9768363 e 9768387).

Su tali soggetti, titolari del trattamento, ricadono, infatti, le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati, avendo comunque una "responsabilità generale" sui trattamenti posti in essere anche quando talune operazioni di trattamento siano poste in essere da un responsabile del trattamento per loro conto, sulla base delle istruzioni impartite dai soggetti titolari (cons. 79 e 81, art. 5, par. 2, che formalizza il c.d. principio di "responsabilizzazione", 24 e 28 del Regolamento; cfr., tra i tanti, provv. 10 febbraio 2022, n. 43, doc. web n. 9751498 e i precedenti provv. ivi richiamati; v. anche le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. par. 174).

Il titolare può pertanto affidare lo svolgimento di alcune attività di trattamento a un responsabile – che presenti garanzie sufficienti sulla messa in atto di misure tecniche e organizzative idonee a garantire che il trattamento sia conforme alla disciplina in materia di protezione dei dati personali (cfr. cons. 81 e art. 28, par. 1, del Regolamento) – disciplinando il relativo 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 caso in questione, "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 Regolamento disciplina, inoltre, gli altri specifici obblighi e le altre forme di cooperazione cui è tenuto il responsabile del trattamento e l'ambito delle responsabilità che incombono rispettivamente sul titolare e sul responsabile (v. artt. 30, 32, 33, par. 2, 82 e 83 del Regolamento).

In tale quadro, quindi, il responsabile del trattamento è, in ogni caso, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare" (art. 28, par. 3, lett. a), del Regolamento), dovendo assistere quest'ultimo nel garantire il rispetto degli obblighi derivanti dalla disciplina di protezione dati, "tenendo conto della natura del trattamento" e dello specifico regime giuridico applicabile allo stesso (art. 28, par. 3, lett. f), del Regolamento).

Con riguardo al caso di specie si rileva, pertanto, che la decisione di avvalersi dei servizi offerti da una società esterna, anziché realizzare in autonomia un applicativo per l'acquisizione e gestione delle segnalazioni di illeciti, discende da una precisa scelta del titolare del trattamento che tratta i dati personali in tale ambito per adempiere a un obbligo di legge derivante dal predetto quadro normativo in materia di whistleblowing.

Sebbene la Società abbia dichiarato che nessun dato relativo alle segnalazioni è stato reso accessibile neppure "al personale interno all'azienda", essendosi limitata, nel fornire l'applicativo in questione, a effettuare talune operazioni, quali, in particolare, "la manutenzione sistemistica automatica per garantire il back-up del server" e "gli aggiornamenti applicativi nel caso di evoluzione normativa", si osserva che le informazioni presenti all'interno delle segnalazioni di condotte illecite acquisite mediante l'applicativo in questione, comunque "installato su server presso il data center della Società", seppur sottoposti a cifratura, devono essere considerati come dati personali. La cifratura dei dati costituisce, infatti, un'efficace misura che il titolare e il responsabile, anche in base ai principi della protezione dei dati fin dalla progettazione e per impostazione predefinita, possono adottare per rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi – garantendo la sicurezza del trattamento e tutelando i diritti e le libertà degli interessati – ma non è di per sé idonea a rendere le informazioni cifrate non più riferibili a una persona identificata o identificabile (cfr. cons. 83, e artt. 4, punto 1), 25 e 32, par. 1, lett. a), del Regolamento, v., da ultimo, provv. 7 aprile 2022, n. 135, doc. web n. 9768387).

Pertanto, le funzioni svolte dalla Società hanno comportato un trattamento dei dati personali dei segnalanti e degli altri interessati indicati nelle segnalazioni (soggetti segnalati, testimoni, ecc.), di cui ciascuno dei suoi clienti risulta comunque titolare, trattandoli in base ad un preciso obbligo di legge.
In tali casi la disciplina in materia di protezione dei dati, come detto, richiede che il rapporto tra il titolare e il fornitore sia regolato da un contratto o da altro atto giuridico ai sensi dell'art. 28 del Regolamento (v. anche considerando 81 e art. 4, punto 8, del Regolamento), anche al fine di evitare trattamenti 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, che definisce la "comunicazione" di dati personali.

Ciononostante, con riguardo al caso di specie, il rapporto tra alcuni clienti (Comune di Ginosa e Acqua Novara.VCO S.p.a.) e la Società non è stato regolato sotto il profilo della protezione dei dati, ai sensi dell'art. 28 del Regolamento.

Alle contestazioni formulate dal Garante, la Società ha replicato che, con riguardo ai rapporti con i predetti clienti, "non si sia provveduto all'adeguamento all'art. 28 del Regolamento con un'investitura "formale" di CLIO a Responsabile del trattamento a latere del Contratto di fornitura" ma che in concreto tale contratto "implicava de facto un tale ruolo da parte del fornitore". Al riguardo, si ribadisce che, in base alla disciplina di protezione dei dati, quando si avvale di un responsabile per lo svolgimento di talune attività di trattamento, il titolare affida compiti analiticamente specificati per iscritto al responsabile e vigila altresì sulla loro osservanza.

Il responsabile, a propria volta, effettua tali trattamenti attenendosi alle istruzioni impartite dal titolare e può, pertanto, legittimamente trattare i dati personali per conto del titolare solo sul presupposto di un contratto o altro atto giuridico, la cui sussistenza non costituisce, contrariamente a quanto sostenuto dalla Società, un mero adempimento formale, dovendo esso

disciplinare taluni tra i più rilevanti aspetti del trattamento e recepire le specifiche istruzioni del titolare. Ne consegue che, più in generale, il trattamento può in ogni caso legittimamente avvenire da parte del responsabile, solo in presenza di idonea regolamentazione del rapporto sotto il profilo della protezione dei dati ed entro i limiti e con le modalità dettate dal titolare per l'esecuzione del trattamento dei dati (cfr. art. 28, par. 5, del Regolamento).

Tali principi trovavano applicazione anche con riguardo al quadro giuridico antecedente al Regolamento, come precisato dalla Corte di Cassazione (v. Cass., Sez. I Civ., ordinanza n. 21234 del 23 luglio 2021, ancorché in relazione a trattamenti di dati personali in un diverso contesto). Nel confermare un provvedimento del Garante, la Corte, per i profili che rilevano nel caso di specie, ha precisato che "l'accordo intercorrente tra il "titolare" ed il "responsabile" è legislativamente previsto e non è destinato solo a regolare i rapporti inter partes, con valenza meramente interna, sotto il profilo dell'eventuale inadempimento contrattuale - come erroneamente sostiene la ricorrente -, perché la disciplina ivi dettata dal "titolare", in merito alle finalità e alle modalità del trattamento, assurge ad elemento necessario per la qualificazione di "responsabile" nel caso concreto".

Come già in precedenza chiarito dal Garante con riguardo ad analoghe fattispecie, non essendo stata individuata come responsabile del trattamento e non essendo stati indicati da parte della Società specifici presupposti che abbiano legittimato il trattamento dei dati personali, si deve concludere che lo stesso è stato effettuato in assenza delle condizioni di liceità previste dal Regolamento e dal Codice. L'art. 6, par. 1, lett. c), del Regolamento, infatti, ammette il trattamento se necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" e legittima il titolare del trattamento, tenuto all'osservanza dell'obbligo, a trattare i dati per tale finalità e non altri soggetti che trattano i dati per conto del titolare (sul punto, con riguardo al difetto di legittimazione del trattamento per i soggetti che trattano i dati per conto e nell'interesse del titolare del trattamento, in caso di mancata regolamentazione del rapporto ai sensi dell'art. 28 del Regolamento, v. provv. 17 settembre 2020, nn. 160 e 161, doc. web nn. 9461168 e 9461321; v. anche provv. 11 febbraio 2021, n. 49, doc. web n. 9562852, provv. 17 dicembre 2020, nn. 280, 281 e 282, doc. web nn. 9524175, 9525315 e 9525337, nonché provv. 10 febbraio 2022, nn. 43 e 44, doc. web n. 9751498).

Alla luce delle considerazioni che precedono, nel caso in esame, non essendo stata individuata la Società come responsabile del trattamento, in assenza della prescritta "istruzione documentata" da parte del titolare (art. 28, par. 3, lett. a), del Regolamento), e non essendo stati rinvenuti specifici e autonomi presupposti di liceità per legittimare il trattamento dei dati personali da parte della stessa, si deve concludere che il trattamento dei dati personali contenuti nelle segnalazioni di presunti illeciti acquisite tramite il predetto applicativo è stato effettuato in assenza delle condizioni di liceità previste dal Regolamento e dal Codice, in violazione degli artt. 5, par. 1, lett. a), e 6 del Regolamento e dell'art. 2-ter del Codice.

Pur tenendo in considerazione la circostanza che, successivamente alle attività ispettive, la Società ha provveduto a sollecitare i propri clienti al fine di ottenere la regolamentazione dei relativi rapporti sotto il profilo della protezione dei dati, si ritiene che tale circostanza non possa essere ritenuta sufficiente ai fini dell'esclusione della responsabilità della Società in ordine all'effettuazione di trattamenti di dati personali, anteriormente alla disciplina di tali trattamenti ai sensi dell'art. 28 del Regolamento.

3.2. Mancata tenuta del registro delle attività di trattamento svolte per conto dei titolari del trattamento.

Il Regolamento prevede, tra gli obblighi generali connessi alle attività di trattamento dei dati personali, anche quello, gravante in capo a ogni titolare del trattamento e responsabile del trattamento (per le attività poste in essere per conto del titolare), di redigere dei "registri delle attività di trattamento" (art. 30 del Regolamento).

Tali registri, idonei a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione e/o dei trattamenti svolti per conto del titolare del trattamento, sono indispensabili per consentire di valutare e documentare la conformità dei trattamenti alla disciplina in materia di protezione dei dati personali e dunque sono preliminari rispetto all'avvio degli stessi (cfr. sul punto, provv. 7 aprile 2022, n. 134, doc. web n. 9768363, cit.).
Con riguardo al caso di specie, è stata accertata la mancata tenuta del registro delle attività di trattamento svolte per conto dei propri clienti, titolari del trattamento, nell'ambito della gestione dell'applicativo per l'acquisizione e la gestione delle segnalazioni di condotte illecite, in violazione dell'art. 30, par. 2, del Regolamento.

Per tali ragioni, si deve ritenere che, fino alla predisposizione del predetto registro, la Società non ha adempiuto all'obbligo di cui all'art. 30, par. 2, del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dalla Società 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 responsabile 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.

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 – data la natura permanente degli illeciti contestati – deve individuarsi nel momento della cessazione della condotta. Si ritiene che 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 assenza di un'idonea base giuridica, in violazione degli artt. 5 e 6 del Regolamento e dell'art. 2-ter del Codice, e senza tenere il registro delle attività di trattamento svolte per conto dei titolari del trattamento, in violazione dell'art. 30, par. 2, del Regolamento.

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, con riguardo ai trattamenti di dati effettuati per conto dei propri clienti, 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 la Società ha fornito ampia collaborazione nel corso dell'istruttoria, provvedendo a sollecitare i propri clienti a regolare il relativo rapporto ai sensi dell'art. 28 del Regolamento e adottando misure volte ad assicurare che, anche con riguardo ai futuri clienti, sia sempre garantita la corretta definizione di ruoli e responsabilità nel trattamento dei dati, nonché predisponendo il registro delle attività di trattamento svolte per conto dei propri clienti, titolari del trattamento, ed è stato infine considerato il bilancio di esercizio. Non risultano, inoltre, precedenti violazioni commesse dalla Società o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si determina l'ammontare della sanzione pecuniaria, nella misura di euro 10.000,00 (diecimila) per la violazione degli artt. 5, 6 e 30 del Regolamento nonché 2-ter del Codice, atteso che, in relazione al caso specifico, la sanzione risulta effettiva, proporzionata e dissuasiva (art. 83, par. 1, del Regolamento).

Tenuto conto della particolare natura dei dati personali oggetto di trattamento e dei connessi rischi per i segnalanti 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 da Clio s.r.l. per la violazione degli artt. 5, 6 e 30 del Regolamento nonché dell'art. 2-ter del Codice nei termini di cui in motivazione;

ORDINA

a Clio s.r.l., in persona del legale rappresentante pro-tempore, con sede legale in via 95° Reggimento Fanteria 70, 73100 Lecce, C.F./P.IVA 02734350750, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 10.000,00 (diecimila) 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 Clio s.r.l. di pagare la somma di euro 10.000,00 (diecimila) 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