Ordinanza ingiunzione nei confronti di Acqua Novara.VCO S.p.a. - 21 luglio 2022 [9813326]

[doc. web n. 9813326]

Ordinanza ingiunzione nei confronti di Acqua Novara.VCO S.p.a. - 21 luglio 2022

Registro dei provvedimenti
n. 269 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 da Acqua Novara.VCO S.p.a. (di seguito "ANVCO" o "Società").

2. L'attività istruttoria.

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

> Clio ha fornito un elenco dei clienti, tra la Società, 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 responsabile del trattamento unicamente da alcuni clienti, mentre altri, tra cui la Società, "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 di informazioni da parte dell'Ufficio, il Fornitore, in data XX, ha ulteriormente precisato che il rapporto con ANVCO – per la 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 ad ANVCO, 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 ANVCO 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; e non avendo comunicato al Garante i dati di contatto del responsabile della protezione dei dati, in violazione dell'art. 37, par. 7, del Regolamento.

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

> "ANVCO gestisce il servizio idrico integrato in 140 Comuni delle Province di Novara e del Verbano-Cusio-Ossola ed è presente sul territorio con 14 sedi operative. ANVCO è una società in controllo della P.A. e in quanto tale ha adottato sia i sistemi di prevenzione della corruzione, sia il modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001, come da disposizioni ANAC tempo per tempo succedutesi in materia. Ciò si premette in quanto, come si dirà, le norme prevenzionistiche di riferimento sono state utilizzate dalla scrivete Società per valutare e giustificare la selezione del sistema e del fornitore, nonché i ruoli privacy dei soggetti coinvolti nel possibile trattamento dei dati personali";
>
> "nel mese di novembre del 2018 un team composto dall'allora responsabile dell'Ufficio IT e dal Responsabile della prevenzione della corruzione e della trasparenza (RPCT) individuava l'applicativo de quo come idoneo a rispondere alle esigenze dell'Ente di gestire efficacemente le segnalazioni whistleblowing";
>
> "l'ordine di acquisto era sottoscritto in data 16 gennaio 2019 […] e agli inizi del mese di giugno del 2019 il Consiglio di Amministrazione di ANVCO provvedeva all'approvazione dell'aggiornamento della policy interna per l'attività di whistleblowing […]. La messa a disposizione dell'applicativo e il rilascio della policy aggiornata erano altresì accompagnati da una attività formativa indirizzata a tutto il personale nella quale si evidenziavano, tra le altre, le garanzie che il quadro normativo vigente offre al segnalante";
>
> "il 3 luglio 2019 entrava effettivamente "in funzione" l'applicativo e, successivamente, in data XX, la scrivente Società riceveva un messaggio di p.e.c. con il quale il fornitore Clio chiedeva la formulazione dell'atto di nomina a responsabile del trattamento. A seguito delle intercorse intese col fornitore, il documento veniva formalizzato in data 3 dicembre 2019";
>
> "la contrattualizzazione con il fornitore avveniva inizialmente – per il periodo intercorrente tra il 3 luglio 2019 e il 3 dicembre 2019 - senza la formalizzazione della nomina di responsabile del trattamento. Tale scelta era assunta a seguito di una analisi del quadro normativo e delle circostanze fattuali che avevano fatto propendere per una "autonoma" titolarità del fornitore stesso";
>
> "da ricerche effettuate all'epoca non si erano infatti rilevati provvedimenti di codesta Illustrissima Autorità in materia, tranne una relazione al parlamento del 2009 in cui si auspicavano provvedimenti normativi che fornissero un supporto di legittimità per i trattamenti ipotizzabili per i sistemi di segnalazione in questione, e una posizione del Gruppo

Articolo 29 ivi citato che – esaminando la possibilità di ricorrere a fornitori esterni – affermava “Le imprese o i gruppi di imprese che affidano a fornitori esterni parte della gestione del sistema di denuncia restano responsabili delle operazioni di trattamento che ne risultano in quanto i fornitori esterni operano unicamente in qualità di incaricati del trattamento ai sensi della direttiva 95/46/CE. I fornitori esterni possono essere imprese che gestiscono call center ovvero imprese o studi legali specializzati nel raccogliere le denunce e incaricati talvolta di svolgere parte delle necessarie attività di verifica”;

“nell’ambito delle valutazioni formulate in seno all’Ente sino al luglio 2019 (e oltre), non si sarebbe mai verificata la circostanza di una apprensione, seppure occasionale, di un dato personale relativo a segnalante / segnalazione, neppure in fase di manutenzione del sistema (essendo il dato cifrato), poiché un eventuale apprensione avrebbe comportato per il suo dipendente (il tecnico manutentore) una responsabilità penale e, per la società fornitrice una responsabilità contrattuale (si sarebbe verificata una insussistenza di misure attese)”;

“l’aver ritenuto che Clio potesse a buon titolo operare in qualità di “autonomo” titolare pareva quindi, alla luce delle ricerche di cui sopra, una soluzione adeguata a rispettare il principio di effettività (incidenza nella determinazione delle modalità del trattamento) e contestualmente un modo per evitare a Clio le ingerenze che il titolare è tenuto a porre in essere verso il responsabile (attraverso istruzioni e controlli per esempio). Tali ingerenze avrebbero ipoteticamente potuto rappresentare minacce alla segretezza e riservatezza dei dati personali del segnalante e nel concreto minare la fiducia dell’utenza in merito all’uso del sistema per quanto meglio spiegato in nota 1 e nella dottrina citata”;

“la determinazione di ANVCO non trovava però riscontro, a fine del novembre 2019, con le considerazioni che l’Illustrissima Autorità aveva formulato in fase di ispezione presso Clio, l’Ente aveva quindi aderito prontamente alla interpretazione proposta, dopo averne ricevuto informazione da Clio, ritenendo che essa – per la prima volta – era una chiara posizione sul tema da parte dell’Autorità. Tale interpretazione era negli stessi giorni ribadita dall’Autorità Garante, con provvedimento del 4 dicembre 2019 (doc. web n. 9215763), in occasione del giudizio favorevole in merito all’adozione di “nuove” Linee Guida da parte di ANAC Nelle Linee Guida ANAC, emanate il 9 giugno 2021 sulla base di quanto previsto dall’art. 54-bis, co. 5, D.lgs. n. 165/2001, sono approfonditi i profili concernenti le segnalazioni effettuate in ambito pubblico, volte a consentire alle amministrazioni e agli altri soggetti destinatari delle stesse di adempiere correttamente agli obblighi derivanti dalla disciplina di protezione dei dati personali. Nel capitolo 2.2. dedicato alla “Modalità di gestione delle segnalazioni: procedure informatizzate e tradizionali” l’ANAC ribadisce, quale modalità prioritaria per tutelare la riservatezza del segnalante, la gestione in via informatizzata delle segnalazioni riconoscendo nel fornitore un ruolo di “autorizzato”, ruolo poi corretto in “responsabile del trattamento””;

“il quadro normativo in cui ANVCO si è trovata ad operare al momento dell’implementazione dell’applicativo di Clio era tutt’altro che definito e la stessa, dopo aver effettuato le ricerche e le considerazioni sopra riportate, aveva ritenuto che la novella legislativa apportata dalla L. n. 179/2017 avesse carattere prevalente su quella di rango regolamentare, come sottolineato anche nel parere n. 615/2020 reso dal Consiglio di Stato sullo schema delle Linee Guida (Consiglio di Stato, Sez. Prima, Adunanza di Sezione del 4 marzo 2020)”;

“le valutazioni effettuate da ANVCO, va ribadito, erano forti anche del fatto che la scelta e le caratteristiche dell’applicativo, descritte analiticamente nel provvedimento dell’Autorità Garante, sono tali da assicurare l’adozione di un elevato livello di sicurezza per i diritti e le libertà degli interessati nel rispetto dei principi di integrità e riservatezza testé descritti anche laddove – in un primo tempo – l’Ente aveva ritenuto il fornitore dell’applicativo quale titolare autonomo del trattamento proprio per le peculiari caratteristiche di indipendenza e

autonomina che tale ruolo assicura, rispetto invece a quello di responsabile del trattamento, figura di per sé vincolata contrattualmente al titolare del trattamento con tutti i conseguenti obblighi che ne discendono, ivi incluso l'assoggettamento ai poteri di istruzione, controllo e trasparenza nei diritti di accesso, riservati dal Regolamento (UE) 2016/679 al gestore dei dati";

"il modello di protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e by default) adottato da ANVCO mediante la scelta della soluzione tecnologica fornita da Clio, implementa infatti misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento effettuato nell'ambito delle procedure informatiche per l'acquisizione e la gestione delle segnalazioni, permettendo che i dati – in primis quelli del segnalante - siano gestiti presso un soggetto terzo diverso dall'amministrazione, in conformità ai principi di segretezza e autonomia dei sistemi che consentano ai lavoratori di segnalare - in condizioni di sicurezza - gli eventuali comportamenti illeciti o sospetti di cui vengano a conoscenza";

"mediante l'applicativo veniva acquisita, nel mese di agosto del 2019, un'unica segnalazione. Alla presa in carico da parte del RPCT tale segnalazione veniva poi archiviata come da relazione che l'ODV ha trasmesso al CdA in data 30 Gennaio 2020";

"si ritiene opportuno evidenziare che, indipendentemente dalle considerazioni sul rapporto tra ANVCO e Clio, eventuali dati personali presenti nell'applicativo: non sono quindi relativi a un segnalante (come inteso dalla L. n. 179/2017), non sono inoltre relativi a un segnalato e/o a illeciti o sospetti di illeciti (sempre come inteso dalla L. n. 179/2017). Infine, non vi è, a conoscenza di chi scrive, evidenza che tali dati personali siano a disposizione di dipendenti / collaboratori di Clio (o di terzi) in quanto la loro eventuale apprensione è tecnicamente scongiurata dalla crittografia, nonché protetta da una previsione di sanzione penale del trasgressore. L'identità (dati personali) del segnalante non è conosciuta nemmeno al RPCT poiché, non sussistendone l'esigenza (la segnalazione non aveva rilevanza penale a valutazione del RPCT e dell'ODV), non è mai stato eseguito l'accesso a detti dati";

"risulta un brevissimo lasso di tempo intercorso tra l'attivazione effettiva del servizio di segnalazione anonima (il XX) e la nomina del fornitore quale responsabile del trattamento dei dati, formalizzata il 3 dicembre 2019";

"l'unica segnalazione dell'agosto 2019 non risultava rilevante ai sensi della L. n. 179/2017 e pertanto risulta ridimensionata notevolmente la gravità oggettiva in relazione alle modalità e al rango del bene giuridico tutelato derivante dalla apprensione delle informazioni su segnalato / segnalante di cui comunque non si ha evidenza";

"con riferimento alla violazione degli artt. 5, par. 1, lett. a), 6 del GDPR e dell'art. 2-ter del Codice Privacy riferita al trattamento illecito di dati personali conseguente alla comunicazione derivante dall'aver messo a disposizione del Fornitore dati relativi alle segnalazioni di illeciti in assenza di un'idonea base giuridica, l'Esponente ritiene che tale fattispecie non si sia nei fatti verificata, essendo i dati personali eventualmente contenuti in essa cifrati ed inaccessibili al fornitore";

la Società "ha provveduto a comunicare nominativo e contatti del RPD sin dalla sua nomina avvenuta nell'anno 2018, trasmettendo l'apposita comunicazione acquisita da codesta Illustrissima Autorità […] Successivamente la ANVCO ha notificato la variazione dei dati del responsabile della protezione dei dati, trasmettendo un'ulteriore comunicazione" in data XX.

In data XX si è, inoltre, svolta l'audizione richiesta da ANVCO, ai sensi dell'art. 166, comma 6, del Codice, in occasione della quale è stato rappresentato, tra l'altro, che:

“la selezione del fornitore del predetto servizio è avvenuta nel mese di dicembre 2018, fornitore con il quale la Società ha stipulato un contratto di servizi nel mese di gennaio 2019; nei mesi successivi, fino al mese di giugno 2019, la Società ha provveduto a effettuare una serie di attività propedeutiche all’attivazione della procedura online di acquisizione e gestione delle segnalazioni, definendo le modalità di utilizzo ed effettuando una campagna di comunicazione e formazione nei confronti di dipendenti”;

“l’attivazione del servizio è avvenuta in data 3 luglio 2019 e nel mese di agosto 2019 è pervenuta una segnalazione che è stata trattata dall’Organismo di vigilanza e dal RPCT e successivamente archiviata”;

“le altre due segnalazioni che risultavano presenti all’interno dell’applicativo whistleblowing all’atto dell’accertamento ispettivo dell’Autorità presso Clio S.r.l., avvenuto nel mese di novembre 2019, sono presumibilmente riconducibili a prove tecniche effettuate dalla Società”;

“le valutazioni effettuate dalla Società in relazione al fornitore del servizio nel trattamento dei dati personali si sono basate sulla qualificata natura dei servizi offerti dallo stesso, nonché dal quadro di settore che prevede specifiche responsabilità penali in caso di divulgazione dell’identità dei segnalanti”;

“la Società, anche a seguito di una specifica richiesta del fornitore successiva all’accertamento ispettivo dell’Autorità, ha poi formalizzato il rapporto con Clio S.r.l. ai sensi dell’art. 28 del Regolamento (UE) 2016/679”.

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).

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).

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).

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).

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 ANVCO, 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, fornitore 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 di ANVCO il quale operava 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 ANVCO 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 la Società e il Fornitore non è stato opportunamente regolato sotto il profilo della protezione dei dati, come risulta dalla documentazione in atti.

In relazione ai profili in materia di protezione dei dati personali, si rileva che il contratto di fornitura del servizio con il fornitore (cfr. all. 1 e 2 alla nota del XX) non ha 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).

Al riguardo non può essere ritenuto rilevante quanto evidenziato nella memoria difensiva circa il riferimento al ruolo assunto dai fornitori esterni in tale ambito, i quali opererebbero "unicamente in qualità di incaricati del trattamento". Tale indicazione è riportata in maniera imprecisa in una traduzione italiana del documento "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime", che invece nella sua versione in lingua inglese qualifica correttamente i fornitori esterni come responsabili del trattamento ("providers merely act as processors"). Ciò, peraltro, non risulta aver in concreto condizionato le valutazioni e le scelte organizzative di ANVCO, atteso che la stessa ha dichiarato di aver ritenuto inizialmente che il Fornitore operasse in qualità di titolare del trattamento.

Risulta pertanto accertato che – ferme restando le valutazioni in ordine alla liceità del trattamento svolto dal Fornitore, oggetto di autonomo procedimento – ANVCO, dal 3 luglio 2019 (data in cui l'applicativo è stato reso pienamente operativo) al 3 dicembre 2019 (data in cui ha regolamentato il rapporto con il Fornitore), ha operato in violazione dell'art. 28 del Regolamento, non avendo disciplinato sotto il profilo della protezione dei dati il rapporto con il Fornitore, in violazione dell'art. 28 del Regolamento.

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 3 luglio al 3 dicembre 2019, stante l'assenza di una regolamentazione del rapporto con il Fornitore ai sensi dell'art. 28 del Regolamento, ANVCO, avvalendosi dei servizi da questo offerti, al fine di dotare la propria struttura di un efficacie ed 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.

Sebbene ANVCO abbia dichiarato che tale trattamento di dati "non si sia nei fatti verificat[o], essendo i dati personali eventualmente contenuti […nella piattaforma] cifrati ed inaccessibili al fornitore" e che "non si sarebbe mai verificata la circostanza di una apprensione, seppure occasionale, di un dato personale relativo a segnalante / segnalazione, neppure in fase di manutenzione del sistema (essendo il dato cifrato)", deve ritenersi che l'utilizzo della cifratura costituisce solo 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. Ciò non esclude, tuttavia, che ricorra nel caso di specie un trattamento di dati personali. Per tali ragioni, stante la definizione di "trattamento" ai sensi dell'art. 4, punto 2), del Regolamento, e come di recente chiarito dal Garante, le informazioni presenti all'interno delle segnalazioni di condotte illecite acquisite

mediante l'applicativo in questione, seppur sottoposti a cifratura, devono essere considerati come dati personali in quanto rappresentano informazioni su persone fisiche identificabili (cfr. cons. 83, e artt. 4, punto 1), 25 e 32, par. 1, lett. a), del Regolamento; sul punto v. provv. 7 aprile 2022, n. 135, doc. web n. 9768387, cit.).

A tal riguardo, non rileva altresì 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, senza che fosse "mai stato eseguito l'accesso" ai dati relativi all'identità del segnalante. Come noto, infatti, anche la sola raccolta e conservazione di dati personali configura un trattamento soggetto alla disciplina in materia di protezione dei dati (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; "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), ANVCO abbia consentito operazioni di trattamento e/o 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, 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. Nel corso del procedimento la Società ha invece comprovato di aver comunicato al Garante i dati di contatto del proprio responsabile della protezione dei dati (ragione per cui si ritiene di dover procedere all'archiviazione del relativo profilo di contestazione).
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, come dichiarato da ANVCO, al momento delle attività ispettive era presente una sola segnalazione di condotte illecite all'interno dell'applicativo in questione e che le violazioni poste in essere si sono protratte per alcuni mesi (dal 3 luglio al 3 dicembre 2019). Inoltre, la Società 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 20.000,00 (ventimila) 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 da Acqua Novara.VCO S.p.a. 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

ad Acqua Novara.VCO S.p.a., in persona del legale rappresentante pro-tempore, con sede legale in via Triggiani Leonardo 9, 28100 Novara, C.F./P. IVA 02078000037, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 20.000,00 (ventimila) 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

ad Acqua Novara.VCO S.p.a., di pagare la somma di euro 20.000,00 (ventimila) 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