Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia - 7 aprile 2022 [9768363]

VEDI NEWSLETTER DELL'11 MAGGIO 2022

[doc. web n. 9768363]

Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia - 7 aprile 2022

Registro dei provvedimenti
n. 134 del 7 aprile 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 dell'Azienda ospedaliera di Perugia (di seguito "Azienda"; v. verbale delle operazioni compiute del XX), sia di ISWEB S.p.A. (di seguito, "Società"), che fornisce e gestisce per conto di numerosi clienti, tra cui l'Azienda, l'applicativo utilizzato per l'acquisizione e la gestione delle segnalazioni di condotte illecite e, a tal fine, è individuata quale responsabile del trattamento (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.

All'esito dell'istruttoria, stante la particolare complessità dei profili di natura tecnologica emersi nel corso dell'istruttoria (cfr. relazione tecnica del XX), è emerso che:

- "l'Azienda, con Deliberazione del Direttore Generale del 22 dicembre 2016, n. 2341, ha adottato, ai sensi della l. 190/2012, il "Regolamento aziendale per la tutela del dipendente che segnala illeciti (whistleblower)" che, all'art. 2, nel precisare l'ambito soggettivo di applicazione dello stesso, chiarisce che i soggetti che possono segnalare sono: dipendenti, collaboratori, consulenti, specializzandi, tirocinanti, frequentatori volontari e tutti i soggetti che, a qualsiasi titolo, svolgono attività all'interno dell'azienda";

- "l'invio di una segnalazione può essere effettuato: (a) in modalità cartacea, a mezzo del servizio postale, inviando il modulo pubblicato sul sito aziendale al Responsabile della prevenzione della corruzione e della trasparenza (RPCT); (b) in modalità verbale direttamene al RPCT; (c) in modalità informatica, avvalendosi di un'applicazione web dedicata";

- "l'Azienda si avvale di una applicazione web gestita e fornita, in modalità cloud, dalla società Internet Soluzioni S.r.l. (ora ISWEB S.p.a.)", il cui rapporto è stato disciplinato ai sensi dell'art. 28 del Regolamento (cfr. la deliberazione del Direttore Generale del 23 settembre 2016, n. 1678, con la quale è stato deliberato l'acquisto della citata applicazione web, nonché l'atto di designazione a responsabile del trattamento della società ISWEB S.p.a. del XX, all. 13 e 16 al verbale del XX; v. anche all. 5 al verbale del XX);

- "il trattamento relativo alla acquisizione e gestione delle segnalazioni di condotte illecite (c.d. whistleblowing) […] non è descritto all'interno del registro dei trattamenti";

- "l'Azienda non ha predisposto un'informativa specifica al riguardo, sebbene un'informativa generale sui trattamenti dei dati personali dei dipendenti sia presente all'interno dei contratti individuali di lavoro" (cfr. all. 18 e 19 al verbale del XX).

- "l'applicazione web, sebbene esposta su rete pubblica all'indirizzo "https://whistleblowing.ospedale.perugia.it/", è raggiungibile esclusivamente da postazioni di lavoro attestate alla rete aziendale";

- "l'Azienda ha reso disponibile sul sito aziendale un manuale operativo che illustra le modalità di invio di una segnalazione mediante l'applicazione web in questione. In particolare, è prevista una prima fase di "Iscrizione nel sistema" da effettuare all'atto della prima segnalazione che prevede l'inserimento di alcuni dati identificativi e di contatto del segnalante, oltre che la qualifica e la sede di servizio. A seguito di questa iscrizione, l'applicazione web mostra al segnalante il c.d. "codice whistleblower" e, contestualmente,

invia un'email al soggetto con il ruolo di "incaricato della gestione dell'anagrafica degli iscritti". Successivamente a tale fase, è possibile inviare una segnalazione tramite la funzione "Fai una segnalazione" che prevede la compilazione di campi relativi alle condotte oggetto di segnalazione e ai soggetti che le hanno poste in essere. A seguito dell'invio della segnalazione, l'applicazione web mostra al segnalante il c.d. "codice segnalazione" che consente di monitorare lo stato di avanzamento della segnalazione, di integrarla e di scambiare messaggi con il RPCT";

- "a seguito dell'invio della segnalazione, l'applicazione web invia un'email al soggetto con il ruolo di "responsabile della prevenzione della corruzione"";

- "l'accesso alla rete pubblica avviene mediante sistemi firewall di nuova generazione, che consentono di configurare specifiche regole di navigazione in internet, anche in ragione del ruolo e delle diverse funzioni svolte dai dipendenti o da altri soggetti che hanno accesso alla rete aziendale […] "tali sistemi firewall memorizzano in appositi file di log le operazioni di navigazione effettuate, unitamente a dati che consentono di risalire anche indirettamente ai dipendenti o ad altri soggetti che le hanno effettuate […] non sono state previste specifiche cautele al fine di non effettuare la registrazione delle operazioni di navigazione sull'applicazione web per l'acquisizione e la gestione di segnalazioni di condotte illecite";

- i "log di navigazione in internet sono conservati in un server virtuale collegato al firewall fino al raggiungimento della dimensione massima del file di log (150 GB) […] al raggiungimento di tale dimensione, i record più vecchi vengono sovrascritti dai record più recenti" e "nell'ambito delle procedure di backup, tali log sono conservati per un ulteriore periodo che l'Azienda ha fatto riserva di comunicare";

- "l'unico soggetto autorizzato al trattamento delle segnalazioni di condotte illecite è il RPCT, incarico che è stato svolto dalla dott.ssa […] dal 2013 al 2 maggio 2019, data a decorrere della quale sono diventate effettive le dimissioni presentate dalla stessa";

- a seguito delle dimissioni del RPCT, "le due credenziali di autenticazione (una per verifica dell'anagrafica dei segnalanti e una per la gestione delle segnalazioni) utilizzate dallo stesso per accedere all'applicativo in questione sono state consegnate da quest'ultimo al responsabile dell'Ufficio prevenzione della corruzione, trasparenza e trattamento dei dati personali all'interno di una busta chiusa";

- le predette "credenziali di autenticazione sono tuttora attive e che la casella di posta elettronica sulla quale l'applicazione web invia le notifiche dell'avvenuta iscrizione di un segnalante e della ricezione di una segnalazione è quella assegnata alla dott.ssa […]";

- l'Azienda ha "dato comunicazione all'ANAC della cessazione dall'incarico di RPCT della dott.ssa […] e di aver successivamente trasmesso alla stessa Autorità il nominativo del nuovo RPCT, incarico assunto in via temporanea ed eccezionale dal dott. […], Direttore amministrativo dell'Azienda"; "la straordinarietà della situazione in cui versa l'Azienda non ha consentito di individuare tra i dirigenti in servizio il RPCT e che è stata avviata un'attività esplorativa volta a individuare un soggetto, preferibilmente esterno, idoneo a ricoprire tale funzione che, ad oggi, non ha ancora avuto un esito positivo";

- "le citate credenziali di autenticazione (una per verifica dell'anagrafica dei segnalanti e una per la gestione delle segnalazioni) non sono ancora state assegnate al nuovo RPCT";

- "l'Azienda Ospedaliera non ha effettuato su tale trattamento la valutazione di impatto ai sensi dall'art. 35 del Regolamento".

Nel corso degli accertamenti effettuati presso la Società la stessa ha dichiarato (cfr. verbali del

XX, pp. 3 e ss.) quanto segue:

- “la società commercializza un servizio basato sul software open source denominato “GlobalLeaks”, curandone l’installazione, la configurazione (sia in fase di attivazione che nel corso del rapporto contrattuale) nonché la manutenzione tecnica dello stesso. Allo stato il servizio è erogato tramite due server dedicati su cui sono installate due differenti versioni del software “GlobalLeaks”: la prima (versione 2.60.113) in produzione dal 2015 e in uso presso la maggior parte dei committenti sarà progressivamente sostituita dalla seconda (versione 3.10.8), più aggiornata, attualmente in uso presso un numero più limitato di committenti”;

- la versione 2.60.113 del software “GlobalLeaks”, in uso anche presso l’Azienda ospedaliera di Perugia (cfr. all. 8 al verbale del XX) “tiene conto delle indicazioni contenute nelle linee guida ANAC del 2015. In particolare, anche al fine di garantire la separazione dei dati identificativi del segnalante dal contenuto della segnalazione, l’applicativo whistleblowing mette a disposizione dei segnalanti due distinte procedure: la prima permette l’iscrizione sull’applicativo con il rilascio del c.d. “codice segnalante”, necessario per l’invio di una segnalazione, mentre la seconda consente l’invio di una segnalazione con il rilascio del c.d. “codice segnalazione”, necessario per verificare lo stato di una segnalazione. L’applicativo whistleblowing mette a disposizione un’interfaccia di back-office tramite la quale le iscrizioni vengono validate dai soggetti con il profilo di “amministratore delle anagrafiche” (che verificano che l’iscritto sia un soggetto titolato a inviare la segnalazione) e le segnalazioni vengono gestite dai soggetti con il profilo di “amministratore delle segnalazioni”” (cfr. anche all. 8 al verbale del XX);

- “le segnalazioni sono pienamente consultabili e gestibili solo dopo la validazione dell’iscrizione del segnalante, anche nei casi in cui siano state trasmesse precedentemente. L’applicativo non prevede l’invio di messaggi di notifica sull’indirizzo e-mail del segnalante, essendo rimessa a questo la possibilità di consultare lo stato della segnalazione mediante il c.d. “codice segnalazione”. Diversamente, l’applicativo prevede l’invio di messaggi di notifica sugli indirizzi e-mail dei soggetti con il profilo di “amministratore delle anagrafiche” e di “amministratore delle segnalazioni””;

- “i soggetti con il profilo di “amministratore delle segnalazioni” (di regola il RPCT) possono avere accesso ai dati identificativi del segnalante previo inserimento di una specifica motivazione che viene registrata sull’applicativo whistleblowing e risulta visibile anche al segnalante in sede di consultazione dello stato della segnalazione”;

- la versione 3.10.8 del software “GlobalLeaks”, “contrariamente alla precedente che prevedeva due diversi moduli per l’iscrizione dei segnalanti e l’invio delle segnalazioni, mette a disposizione dei segnalanti un unico modulo per l’inoltro di una segnalazione di condotte illecite. Nell’ambito di tale procedura, un segnalante può scegliere di rimanere anonimo o di inserire i dati relativi alla sua identità. Anche nel caso di una segnalazione originariamente anonima, il segnalante ha facoltà di accedere all’applicativo whistleblowing mediante il c.d. “codice segnalazione” – generato a seguito dell’invio della segnalazione – per verificare lo stato della stessa ed eventualmente per inserire i dati relativi alla sua identità”;

- “l’applicativo whistleblowing, anche al fine di garantire un’efficace separazione dei dati identificativi del segnalante dal contenuto della segnalazione, prevede uno specifico procedimento per rendere visibili i dati relativi all’identità del segnalante ai soggetti con il profilo di “amministratore delle segnalazioni”. È infatti prevista la possibilità di assegnare il profilo di “custode delle identità” a soggetti che operano sotto l’autorità del titolare del trattamento, ai quali i soggetti con il profilo di “amministratore delle segnalazioni” possono richiedere, previo inserimento di una congrua motivazione, l’accesso ai dati relativi all’identità del segnalante. I soggetti con il profilo di “custode delle identità” non hanno

accesso né ai dati relativi all'identità del segnalante né al contenuto della segnalazione ma possono visualizzare unicamente la motivazione associata alla richiesta di accesso ai dati relativi all'identità del segnalante";

- "tra le varie personalizzazioni consentite dall'applicativo whistleblowing, è possibile: (1) il soggetto con il profilo di "amministratore delle segnalazioni" possa anche inviare file al segnalante; (2) il soggetto con il profilo di "amministratore delle segnalazioni" può in autonomia effettuare le operazioni di export, di cancellazione, di disabilitazione delle notifiche e di prolungamento del termine predefinito di "scadenza della segnalazione" (allo scadere del quale i dati della segnalazione vengono cancellati in modo sicuro); (3) il soggetto con il profilo di "amministratore del tenant" può, nel configurare i c.d. "questionari" che definiscono la struttura del modulo di segnalazione, definire delle regole per consentire la visibilità di una specifica tipologia di segnalazione ad specifico soggetto con il profilo di "amministratore delle segnalazioni" (es. un collaboratore dello staff assegnato al RPCT)";

- "le misure di sicurezza adottate a protezione dei dati trattati con l'ausilio dell'applicativo whistleblowing" sono descritte in appositi documenti forniti dalla Società (cfr. all. 2 e 3 al verbale del XX);

- "il software "GlobalLeaks" utilizza protocolli sicuri per il trasporto dei dati (https) e strumenti di crittografia per la conservazione dei dati (contenuti delle segnalazioni ed eventuale documentazione allegata), descritti anche nel documento che descrive le misure di sicurezza dell'applicativo whistleblowing" (cfr. all. 2 al verbale del XX);

- "è previsto il tracciamento, in appositi file di log, degli accessi e delle operazioni compiute sull'applicativo whistleblowing dai soggetti con il profilo di "amministratore delle anagrafiche" e di "amministratore delle segnalazioni". Con riferimento agli accessi e alle operazioni compiute dai segnalanti, l'applicativo whistleblowing non conserva, nei file di log, l'indirizzo IP del dispositivo utilizzato dagli stessi";

- "ISWEB ha predisposto una valutazione d'impatto sulla protezione dei dati relativa ai trattamenti dei dati personali svolti dalla società e che rende disponibile ai propri clienti" (cfr. all. 4 al verbale del XX);

- l'Azienda ospedaliera di Perugia ha richiesto alla Società di effettuare le "modifiche necessarie a seguito della nomina di un nuovo responsabile della prevenzione della corruzione e della trasparenza (RPCT)" (cfr. corrispondenza intercorsa, all. 6 al verbale del XX);

- "la società ha affidato alla società Seeweb S.r.l. il servizio di hosting dei sistemi informatici che ospitano, tra gli altri, l'applicativo whistleblowing, fornendo il contratto e la "Descrizione servizi e GDPR Compliance" […], documenti da cui si evincono i ruoli delle due società nel trattamento dei dati personali" (cfr. all. 7 al verbale del XX; v. atto di nomina di Seeweb s.r.l., allegato alla successiva nota del XX).

Con nota del XX, l'Ufficio, sulla base degli elementi acquisiti, ha notificato all'Azienda, 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 l'Azienda 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, in maniera non conforme ai principi di "liceità, correttezza e

trasparenza” e senza fornire agli interessati le informazioni relative al trattamento, in violazione degli artt. 5, par. 1, lett. a), 13 e 14 del Regolamento; in maniera non conforme ai principi di “integrità e riservatezza”, della “protezione dei dati fin dalla progettazione” e della “protezione dei dati per impostazione predefinita”, in violazione degli artt. 5, par. 1, lett. f), e 25 del Regolamento; in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, in violazione dell’art. 32 del Regolamento; non avendo riportato nel registro dei trattamenti le attività di acquisizione e gestione delle segnalazioni di condotte illecite, in violazione dell’art. 30 del Regolamento; non avendo effettuato una valutazione d’impatto sulla protezione dei dati, in violazione dell’art. 35 del Regolamento.

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

- “all'epoca dell'espletamento delle attività ispettive […] l’Azienda era stata investita da una inchiesta giudiziaria che […] ha, di fatto, stravolto l'assetto organizzativo interno all'Azienda, impedendole di svolgere in modo accurato e tempestivo molte delle proprie attività amministrative ordinarie […] In tale contesto l' Azienda ha comunque svolto le proprie funzioni principali (prima fra tutte la tutela della salute del cittadino) e si è trovata, suo malgrado, costretta ad adottare, talvolta, alcune precarie soluzioni”;

- “Tale contesto, quindi, ha influito pesantemente sulle questioni che l’Autorità contesta nel proprio verbale e non se ne potrà non tenerne conto in quanto non si è trattato di una situazione "ordinaria" ma di una delle più importanti inchieste giudiziarie degli ultimi 30 anni della Regione Umbria con un "azzeramento" della classe dirigente e delle posizioni apicali di questa Azienda”;

- “Com'è noto, la pandemia Covid-19 ha investito il nostro Paese (ed il resto del mondo) sin dal Febbraio 2020 […] L' Azienda Ospedaliera di Perugia rappresenta il più importante Ospedale della Regione Umbria e presso di esso confluiscono gran parte dei malati Covid. […] Questa situazione di emergenza sanitaria ha impegnato pesantemente tutta l'organizzazione dell'Ospedale, sia essa sanitaria che amministrativa, con difficoltà organizzative interne ed un aggravio di costi e di spese di cui non si potrà non tenerne conto”;

- "nessuna segnalazione [... di condotte illecite] è mai giunta al sistema deputato dall'Azienda ad inviare e ricevere dette segnalazioni. Tale aspetto non può ritenersi secondario in quanto al momento dell'ispezione, ma anche successivamente, nessun trattamento di dati personali né di informazioni riservate si è concretizzato e pertanto, dal punto di vista di tutela sostanziale, nessun trattamento illecito o trattamento non conforme può ritenersi realizzato”;

- con riguardo al “mancato assolvimento dell'obbligo di rendere informazioni agli interessati” si precisa che “nella sezione a ciò deputata era presente, già all'epoca dell'ispezione, una parte introduttiva in cui veniva specificata la funzione della segnalazione e l'anonimato garantito del segnalante” successivamente “nella suddetta sezione [è stata inserita] un'informativa strutturata ricavabile dal link https://www.ospedale.perugia.it/pagine/segnalazione-illeciti-whistleblowing [... ed è stata affissa anche] nei luoghi di lavoro e/o in bacheca aziendale”;

- “si è proceduto ad integrare il registro del trattamento con la sezione dedicata al whistleblowing”;

- “il sistema firewall all'epoca in essere pur registrando l'indirizzo IP e le credenziali

dell'utente non rilevava le attività che lo stesso avrebbe potuto effettuare dopo l'accesso alla pagina web deputata https://whistleblowing.ospedale.perugia.it/. Inoltre l'accesso alla consultazione dei log poteva essere effettuato esclusivamente dall'Amministratore di Sistema (circostanza peraltro mai avvenuta). Si precisa che a seguito dell'ispezione di codesta Autorità, l'Azienda ha operato una modifica sostanziale: l'accesso alla pagina web https://whistlerblowing.ospedale.perugia.it/ è stato escluso dalla registrazione dei log e quindi non è possibile risalire a nessun dato di accesso";

- "le credenziali di autenticazione del RPCT dimissionario [...] rimasero attive in quanto le dimissioni del suddetto soggetto Responsabile non furono formalmente accolte e recepite sino alla nomina del successivo RPCT individuato nella persona del Direttore Amministrativo";

- "al momento della decisione circa le necessità di adottare una valutazione d'impatto sul trattamento dei dati personali relativi alle possibili segnalazioni di illecite condotte fu deciso di considerare sufficiente, a quel momento, la DPIA - Data Protection Impact Assesment realizzata dal fornitore del software di gestione del programma di whistleblowing "Isweb""; nel corso dell'istruttoria l'Azienda "ha deciso di adottare una specifica DPIA".

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

- "dal 1° gennaio 2021 [...] sono state avviate diverse iniziative volte anche a migliorare la governance dei processi aziendali relativi all'anticorruzione e alla protezione dei dati personali";

- "non c'è stata alcuna violazione dei dati personali in quanto non è stata acquisita e trattata alcuna segnalazione di condotte illecite mediante l'applicativo whistleblowing oggetto degli accertamenti ispettivi";

- "l'Azienda sta partecipando attivamente alla redazione di un codice di condotta di settore, promosso dall'ALTEMS dell'Università Cattolica del Sacro Cuore" e ha svolto numerosi corsi di formazione e "sono in programma ulteriori corsi di formazione del personale dipendente, nell'ambito dei quali sono previste specifiche sessioni di formazione sull'utilizzo dell'applicativo whistleblowing".

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 ex 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).

Numerosi sono stati, in questi anni, gli interventi anche di carattere generale in materia (cfr., 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) e decisioni su singoli casi (v. provv.ti 10 giugno 2021, n. 235, doc. web n. 9685922, e n. 236, doc. web n. 9685947; cfr. newsletter n. 480 del 2 agosto 2021, doc. web n.

9687860, ma già provv. 23 gennaio 2020, n. 17, doc. web n. 9269618; newsletter n. 462 del 18 febbraio 2020, doc. web n. 9266789); da ultimo, il Garante nel corso di un'audizione in Parlamento 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 ddl di delegazione europea 2021- Senato della Repubblica-14esima Commissione parlamentare dell'Unione europea, 8 marzo 2022, doc. web n. 9751458).

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, l. n. 179/2017 che ha aggiunto il comma 2-bis all'art. 6 del d.lgs. 8 giugno 2001, n. 231).

Il quadro normativo sopra richiamato – che ha aggiornato la precedente disciplina sotto diversi profili, dal quadro sanzionatorio (cfr. art. 54-bis, comma 6, cit.), alle tutele specifiche per l'interessato, quali la reintegrazione nel posto di lavoro in caso di licenziamento "a motivo della segnalazione" e la nullità di eventuali "atti discriminatori o ritorsivi" (art. 54-bis, commi 7 e 8, cit.) –, prevede, più in generale, misure volte a proteggere la divulgazione dell'identità del segnalante, allo scopo di prevenire l'adozione di misure discriminatorie nei confronti dello stesso. In tale quadro, infatti, "l'identità del segnalante non può essere rivelata" (art. 54-bis, comma 3, cit.), con alcuni contemperamenti (cfr. art. 54-bis, commi 3 e 9, cit., in relazione ai procedimenti penali, contabili o disciplinari che dovessero conseguire alla segnalazione o "nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la [segnalazione o se è accertata] la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave"). La segnalazione è inoltre sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni (art. 54-bis, comma 4, cit.).

Stante l'art. 54-bis, comma 5, che prevede l'adozione da parte dell'ANAC, sentito il Garante, di apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni, il Garante, con provvedimento del 4 dicembre 2019 (doc. web n. 9215763), ha reso il proprio parere sullo schema di linee guida, confermando che la disciplina di settore in materia di whistleblowing deve essere coordinata, in sede applicativa, con la normativa in materia di protezione dei dati personali. Pertanto, i soggetti obbligati al rispetto delle richiamate disposizioni devono trattare i dati necessari all'acquisizione e gestione delle segnalazioni anche nel rispetto della disciplina di protezione dei dati personali.

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 (artt. 6, par. 1, lett. c), 9, par. 2, lett. b), e 10 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, n. 235, doc. web n. 9685922, e n. 236 doc. web n. 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).

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. Mancato assolvimento dell’obbligo di rendere informazioni agli interessati.

Con riguardo al principio di “liceità, correttezza e trasparenza” il titolare ha l’obbligo di fornire preventivamente a tutta la platea dei possibili soggetti interessati specifiche informazioni sul trattamento dei dati personali e deve adottare “misure appropriate per fornire all’interessato tutte le informazioni di cui agli articoli 13 e 14 […]” del Regolamento (art. 12 del Regolamento).

Tuttavia, nel corso dell’attività istruttoria, l’Azienda ha dichiarato di non aver reso una specifica informativa preventiva in relazione ai trattamenti derivanti dall’acquisizione di segnalazioni di presunti illeciti, né le informazioni sul trattamento richieste dagli artt. 13 e 14 Regolamento risultano altrimenti rese dall’Azienda, non essendo, ad esempio, incluse nell’atto organizzativo adottato dal titolare per la gestione delle segnalazioni, o pubblicate in un’apposita sezione dell’applicativo informatico utilizzato per l’acquisizione e gestione delle segnalazioni, o, ancora, nei contratti individuali di lavoro.

Né può essere ritenuta sufficiente la circostanza rappresentata in sede di memorie difensive in base alla quale “nella sezione a ciò deputata era presente, già all'epoca dell'ispezione, una parte introduttiva in cui veniva specificata la funzione della segnalazione e l'anonimato garantito del segnalante”. Tali iniziative non possono sostituire l’informativa che il titolare deve rendere, prima di iniziare il trattamento, agli interessati in merito alle caratteristiche essenziali dello stesso (cfr. Sentenza della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 - Ricorso n. 61496/08 - Causa Barbulescu c. Romania, spec. n. 140).

Si dà atto che nel corso del procedimento l’Azienda ha provveduto a redigere un’informativa dedicata ai trattamenti connessi all’acquisizione e gestione delle segnalazioni di condotte illecite, come documentato in occasione delle memorie difensive (cfr. all. A alla nota del XX).
Per tali ragioni, fino all’adozione del nuovo documento informativo relativo ai trattamenti in questione, messo a disposizione degli interessati, l’Azienda non ha operato conformemente al principio di correttezza e trasparenza e dunque in violazione degli artt. 5, par. 1, lett. a), 13e 14 del Regolamento.

3.2. Mancata indicazione dei trattamenti per finalità di whistleblowing nel registro delle attività di trattamento

L'art. 30 del Regolamento prevede tra gli adempimenti principali del titolare del trattamento la tenuta del registro delle attività di trattamento, che deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. La tenuta del registro, che deve contenere le principali informazioni relative alle operazioni di trattamento svolte, è funzionale al rispetto del principio di "responsabilizzazione" del titolare (art. 5, par. 2, del Regolamento), in quanto costituisce uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione del titolare. Ciò risulta particolarmente rilevante con riguardo alle attività di valutazione e di analisi del rischio, costituendo, pertanto, un adempimento preliminare rispetto a tali attività.

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare, tra le quali le finalità del trattamento (art. 30, par. 1, lett. b)) anche, se del caso, con l'indicazione della relativa base giuridica. Nel caso di specie, invece, come verificato nel corso dell'attività ispettiva e confermato dall'Azienda, i trattamenti di dati personali effettuati per finalità di acquisizione e gestione di segnalazioni di condotte illecite (c.d. whistleblowing) non risultavano censiti nel registro delle attività di trattamento.

Si dà atto che nel corso del procedimento l'Azienda ha provveduto a integrare il predetto registro con riferimento ai trattamenti connessi all'acquisizione e gestione delle segnalazioni di condotte illecite, come documentato in occasione delle memorie difensive (cfr. all. B alla nota del XX).

Per tali ragioni, si deve ritenere che, fino all'aggiornamento del registro delle attività di trattamento, l'Azienda non ha adempiuto al predetto obbligo, in violazione dell'art. 30 del Regolamento.

3.3. Tracciamento degli accessi all'applicativo.

Nel corso dell'istruttoria è stato constatato che l'applicativo per l'acquisizione e la gestione delle segnalazioni di condotte illecite, raggiungibile all'indirizzo "https://whistleblowing.ospedale.perugia.it/", è accessibile esclusivamente da postazioni di lavoro attestate alla rete aziendale e che "l'accesso alla rete pubblica [da tali postazioni di lavoro] avviene mediante sistemi firewall di nuova generazione" (cfr. verbale del XX, pp. 5 e 6). Inoltre, è emerso che "tali sistemi firewall memorizzano in appositi file di log le operazioni di navigazione effettuate, unitamente a dati che consentono di risalire anche indirettamente ai dipendenti o ad altri soggetti che le hanno effettuate". Peraltro, è emerso che "non sono state previste specifiche cautele al fine di non effettuare la registrazione delle operazioni di navigazione sull'applicazione web per l'acquisizione e la gestione di segnalazioni di condotte illecite" (cfr. verbale del XX, p. 6).

Al riguardo, l'Azienda ha precisato che "tali log di navigazione in internet sono conservati in un server virtuale collegato al firewall fino al raggiungimento della dimensione massima del file di log (150 GB) e che, al raggiungimento di tale dimensione, i record più vecchi vengono sovrascritti dai record più recenti". Inoltre, "nell'ambito delle procedure di backup, tali log sono conservati per un ulteriore periodo" (cfr. verbale del XX, p. 6). Successivamente, l'Azienda ha comunicato di aver "provveduto ad ampliare lo spazio di archiviazione per garantire il salvataggio degli ultimi tre mesi completi" (cfr. nota del XX).

Come risulta dalla documentazione acquisita nel corso degli accertamenti ispettivi, i log generati dai predetti apparati firewall contengono, tra gli altri, l'indirizzo IP della postazione di lavoro utilizzata per la connessione all'applicativo in questione e la username del soggetto ha effettuato tale connessione.

Ciò posto, si rileva che la registrazione e la conservazione, nei log degli apparati firewall, delle

informazioni relative alle connessioni all'applicativo in questione consente la tracciabilità dei soggetti che utilizzano tale applicativo, tra i quali i segnalanti. Ciò, considerato anche l'esiguo numero di connessioni all'applicativo in questione, rende inefficaci le altre misure adottate per tutelare la riservatezza dell'identità dei segnalanti. Per tali ragioni, la registrazione e la conservazione, all'interno dei log degli apparati firewall, di informazioni direttamente identificative degli utenti dell'applicativo in questione non risulta conforme alle disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32 del Regolamento che stabilisce che il titolare del trattamento debba mettere in atto misure per "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (par. 1, lett. b)) e che "nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (par. 2).

Inoltre, si osserva che, in base al principio della "protezione dei dati fin dalla progettazione" (art. 25, par. 1, del Regolamento), il titolare del trattamento deve adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e deve integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati. Tale obbligo si estende anche ai trattamenti svolti per mezzo di un responsabile del trattamento. Infatti, le operazioni di trattamento effettuate da un responsabile dovrebbero essere regolarmente esaminate e valutate dal titolare per garantire che continuino a rispettare i principi e permettano al titolare di adempiere gli obblighi previsti dal Regolamento (cfr. "Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 7 e 39). Pertanto, la mancata adozione delle predette misure – volte ad attuare i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento – si pone anche in contrasto con il principio della "protezione dei dati fin dalla progettazione" di cui all'art. 25, par. 1, del Regolamento.

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

Come messo in evidenza di recente dal Garante, proprio nell'ambito dei trattamenti effettuati mediante applicativi per l'acquisizione e gestione delle segnalazioni illecite, il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve eseguire, anche avvalendosi del supporto del responsabile della protezione dei dati ove nominato, una valutazione dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica, non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento, in particolare, la disciplina in materia di whistleblowing (v. provv. 10 giugno 2021, n. 235, doc. web n. 9685922, spec. par. 3.2, e provv.ti ivi richiamati), ma anche le norme nazionali che disciplinano le condizioni per l'impiego degli strumenti tecnologici sul posto di lavoro (sotto tale ultimo profilo, con riguardo a operazioni di tracciamento delle connessioni a siti Internet da parte di dipendenti, v. da ultimo provv. 13 maggio 2021, n. 190, doc. web n. 9669974).

Al riguardo, non rileva, ai fini della valutazione complessiva del rispetto degli obblighi di sicurezza del trattamento, quanto evidenziato dalla Società in ordine al fatto che "pur registrando l'indirizzo IP e le credenziali dell'utente" l'apparato firewall "non rilevava le attività che lo stesso avrebbe potuto effettuare dopo l'accesso alla pagina web deputata https://whistleblowing.ospedale.perugia.it/" e che "l'accesso alla consultazione dei log poteva essere effettuato esclusivamente dall'Amministratore di Sistema (circostanza peraltro mai avvenuta)" (cfr. nota del XX).

Si dà atto che, nel corso dell'istruttoria, l'Azienda ha dichiarato che "l'accesso alla pagina web https://whistlerblowing.ospedale.perugia.it/ è stato escluso dalla registrazione dei log e quindi non è possibile risalire a nessun dato di accesso" (cfr. nota del XX).

Per tali ragioni, si ritiene che la registrazione e la conservazione, all'interno dei log degli apparati firewall, di informazioni relative alle connessioni all'applicativo in questione da parte degli utenti – anche solo relative al mero accesso e consultazione delle pagine web dell'applicativo – è stata posta in essere, fino al momento in cui il titolare ha provveduto ad adottare le richiamate misure a tutela degli interessati, in violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento.

3.4. Inidoneità delle modalità di gestione delle credenziali di autenticazione in uso al RPCT.

Nel corso dell'istruttoria l'Azienda ha rappresentato che "l'unico soggetto autorizzato al trattamento delle segnalazioni di condotte illecite è il RPCT, incarico che è stato svolto dalla dott.ssa […] dal 2013 al 2 maggio 2019, data a decorrere della quale sono diventate effettive le dimissioni presentate dalla stessa" (cfr. verbale del XX, p. 6).

A seguito delle dimissioni del RPCT, "le due credenziali di autenticazione (una per verifica dell'anagrafica dei segnalanti e una per la gestione delle segnalazioni)" utilizzate dallo stesso per accedere all'applicativo in questione sono state consegnate da quest'ultimo al responsabile dell'Ufficio prevenzione della corruzione, trasparenza e trattamento dei dati personali all'interno di una busta chiusa. Inoltre, l'Azienda ha precisato che le citate credenziali di autenticazione, non ancora assegnate al nuovo RPCT, erano rimaste attive e che "la casella di posta elettronica sulla quale l'applicazione web invia[va] le notifiche dell'avvenuta iscrizione di un segnalante e della ricezione di una segnalazione [… era] quella assegnata alla dott.ssa […]" (cfr. verbale del XX, p. 6).

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, che comporta l'acquisizione e la gestione delle segnalazioni di condotte illecite, che possono contenere al proprio interno dati personali – appartenenti anche a categorie particolari o relativi a condanne penali e reati (artt. 9, par. 1, e 10 del Regolamento) – riferiti o riferibili al segnalante, al soggetto segnalato o a terzi comunque coinvolti nei fatti segnalati, si ritiene che le predette modalità di gestione delle credenziali di autenticazione per l'accesso all'applicativo in questione non risultano adeguate sotto il profilo della sicurezza.

Nel prendere atto che, a seguito degli accertamenti ispettivi, l'Azienda ha, dapprima, richiesto alla Società di sospendere l'invio di e-mail di notifica da parte dell'applicativo in questione e, successivamente, ha chiesto di configurare l'indirizzo di posta elettronica del nuovo RPCT come destinatario delle e-mail di notifica relative agli eventi di iscrizione di un segnalante e di ricezione di una segnalazione (cfr. all. 6 verbale del XX), si rileva, tuttavia, che la mancata disattivazione delle predette credenziali di autenticazione (username e password) – a seguito della perdita delle qualità che consentivano al RPCT dimissionario, a cui tali credenziali erano attribuite, di accedere ai dati personali trattati nell'ambito dell'applicativo – abbia comportato un elevato e ingiustificato rischio per i diritti e le libertà degli interessati, in considerazione delle gravi conseguenze che sarebbero derivate da eventuali accessi non autorizzati ai dati contenuti in segnalazioni di condotte illecite che potevano pervenire nel periodo che va dal 2 maggio 2019 (data a decorrere

dalla quale sono diventate effettive le dimissioni del RPCT) al 2 luglio 2019 (data in cui l'Azienda, con il supporto della Società, ha provveduto a riconfigurare l'applicativo per consentirne l'utilizzo da parte del nuovo RPCT).

Si osserva, infatti, che, allorquando – come nel caso in esame – non sussistono più le condizioni che consentono a un soggetto di accedere a un sistema di trattamento di dati personali e non si provveda tempestivamente a disattivare le credenziali di autenticazione utilizzate dallo stesso (o comunque a renderle inutilizzabili modificando le relative password), possono determinarsi situazioni che rendono possibile a un soggetto non autorizzato di operare, in assenza di una specifica volontà del titolare del trattamento, nell'ambito di tale sistema di trattamento. Tale circostanza è particolare rilevante tenuto conto del particolare regime di riservatezza dell'identità del segnalante prevista dalla legge.

Per tali ragioni, pur tenendo conto delle precisazioni rese dall'Azienda in occasione delle memorie difensive (con specifico riguardo al fatto che "le credenziali di autenticazione del RPCT dimissionario […] rimasero attive in quanto le dimissioni del suddetto soggetto Responsabile non furono formalmente accolte e recepite sino alla nomina del successivo RPCT individuato nella persona del Direttore Amministrativo"), le predette modalità adottate di gestione delle credenziali di autenticazione per l'accesso all'applicativo in questione non risultano conformi alle disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32 del Regolamento che stabilisce che il titolare del trattamento debba mettere in atto misure per "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (par. 1, lett. b)) e che nel "valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (par. 2).

3.5. Mancata esecuzione di una valutazione d'impatto sulla protezione dei dati.

Come risulta dalle evidenze istruttorie in atti, il trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati (cfr. verbale del XX, p. 7).

A tal proposito, si osserva, invece, che, tenuto conto delle indicazioni fornite anche a livello europeo, il trattamento dei dati personali mediante i sistemi di acquisizione gestione delle segnalazioni presenta rischi specifici per i diritti e le libertà degli interessati, considerata anche la particolare delicatezza delle informazioni potenzialmente trattate, la "vulnerabilità" degli interessati nel contesto lavorativo, nonché lo specifico regime di riservatezza dell'identità del segnalante previsto dalla normativa di settore (cfr. artt. 35 e 88 par. 2 del Regolamento; Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679, WP 248 del 4 aprile 2017; v., da ultimo, provv. 10 giugno 2021, n. 235, doc. web n. 9685922, ma già provv. 4 dicembre 2019, doc. web n. 9215763, con il quale il Garante ha reso il parere ad ANAC 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)", ove espressamente si fa rinvio "ai principali adempimenti previsti dalla normativa in materia di protezione dei dati personali (artt. 13, 14, 30, 35 e 36 del Regolamento), anche tenuto conto degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo").

Come chiarito di recente dal Garante proprio con riferimento ai trattamenti effettuati mediante applicativi per l'acquisizione e gestione delle segnalazioni illecite (v. provv. 10 giugno 2021, n. 235, doc. web n. 9685922, spec. par. 3.3), il trattamento dei dati personali effettuati in tale ambito – in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in

termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore (tanto a livello nazionale quanto a livello europeo, cfr., da ultimo, la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione) – presenta rischi specifici per i diritti e le libertà degli interessati.

Ciò, anche considerata, la "vulnerabilità" degli interessati (soggetti segnalanti e segnalati) nel contesto lavorativo (cfr. artt. 35 e 88, par. 2, del Regolamento; "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017; v., da ultimo, provv. 4 dicembre 2019, doc. web n. 9215763, con il quale il Garante ha reso il parere ad ANAC 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)", ove espressamente si fa rinvio "ai principali adempimenti previsti dalla normativa in materia di protezione dei dati personali (artt. 13, 14, 30, 35 e 36 del Regolamento), anche tenuto conto degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo").

Nel prendere atto che, a seguito di specifici approfondimenti svolti nel corso dell'istruttoria, l'Azienda, seppur tardivamente, ha effettuato una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento (cfr. all. D alla nota del XX), si deve concludere che, fino alla predisposizione della stessa, il trattamento è stato effettuato in assenza di una valutazione d'impatto necessaria a individuare misure specifiche per attenuare i rischi derivanti dal trattamento, in violazione dell'art. 35 del Regolamento.

4. Conclusioni.

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

Sebbene come dichiarato, da ultimo, nel corso dell'audizione presso il Garante "non è stata acquisita e trattata alcuna segnalazione di condotte illecite mediante l'applicativo whistleblowing oggetto degli accertamenti ispettivi", l'Azienda ha comunque posto in essere trattamenti di dati personali, come accertato nel corso dell'istruttoria e confermato dall'Azienda stessa (v. paragrafo 3.3 del presente provvedimento), mediante la registrazione e la conservazione, all'interno dei log degli apparati firewall, di informazioni relative alle connessioni all'applicativo in questione da parte degli utenti, anche solo relative al mero accesso e consultazione delle pagine web dell'applicativo.

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

una specifica valutazione d'impatto sulla protezione dei dati, si ritiene che, stante la cessazione dei trattamenti illeciti avvenuta successivamente alla data in cui il Regolamento è divenuto applicabile (cfr. nota del XX nella quale si dà conto delle varie iniziative assunte dal titolare per porre rimedio alle violazioni contestate), 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 in quanto avvenuto in violazione degli artt. 5, par. 1, lett. a) e f), 13, 14, 25, 30, 32 e 35 del Regolamento.

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

In tale quadro, considerando che la condotta ha esaurito i suoi effetti, non ricorrono invece i presupposti per l'adozione di misure correttive, di cui all'art. 58, par. 2, del Regolamento.

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

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

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

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

Ai fini dell'applicazione della sanzione 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 dall'Azienda, al momento delle attività ispettive non erano presenti segnalazioni di condotte illecite all'interno dell'applicativo in questione, circostanza che non vale ad escludere il trattamento dei dati comunque effettuato (v., in particolare, par. 3.3.del presente provvedimento) e che l'Azienda ha prestato una particolare collaborazione 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. Si è inoltre tenuto conto del fatto che specifici chiarimenti in merito alla necessità di effettuare una valutazione di impatto sulla protezione dei dati in relazione ai trattamenti in esame sono stati forniti dal Garante nell'ambito del citato parere reso ad ANAC il 4 dicembre 2019, cioè successivamente all'effettuazione delle attività ispettive presso l'Azienda. Sono state altresì tenute in considerazione la particolare situazione in cui si trovava l'Azienda nel periodo in cui è stata effettuata l'attività istruttoria e le gravi difficoltà, anche sul piano

organizzativo, che le Aziende sanitarie hanno dovuto affrontare nel contesto dell'emergenza epidemiologica da SARS-CoV-2.

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 40.000,00 (quarantamila) per la violazione degli artt. 5, par. 1, lett. a) e f), 13, 14, 25, 30, 32 e 35 del Regolamento.

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 dall'Azienda ospedaliera di Perugia per la violazione degli artt. 5, par. 1, lett. a) e f), 13, 14, 25, 30, 32 e 35 del Regolamento, nei termini di cui in motivazione;

ORDINA

all'Azienda ospedaliera di Perugia, in persona del legale rappresentante pro-tempore, con sede legale in Ospedale Santa Maria della Misericordia Sant'Andrea delle Fratte, 06156 Perugia, codice fiscale/partita IVA 02101050546, , ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 40.000,00 (quarantamila) 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

all'Azienda ospedaliera di Perugia di pagare la somma di euro 40.000,00 (quarantamila) 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, 7 aprile 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei