Ordinanza ingiunzione nei confronti di ISWEB S.p.A. - 7 aprile 2022 [9768387]

VEDI NEWSLETTER DELL'11 MAGGIO 2022

[doc. web n. 9768387]

Ordinanza ingiunzione nei confronti di ISWEB S.p.A. - 7 aprile 2022

Registro dei provvedimenti
n. 135 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);

- "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"".

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)";

- i registri delle attività di trattamento, svolte in qualità di titolare e di responsabile del trattamento, sono tenuti dalla Società in formato elettronico (cfr. all. 1 al verbale del XX);

- "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 alla Società, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, invitando il predetto responsabile del trattamento a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24 novembre 1981).

Con la nota sopra menzionata, l'Ufficio ha rilevato che il trattamento in questione è stato effettuato in assenza di una idonea disciplina del rapporto con Seeweb S.r.l. a cui la Società ha fatto ricorso sia per i trattamenti posti in essere in qualità di titolare, in violazione dell'art. 28, parr. 1 e 3, del Regolamento, sia per quelli effettuati in qualità di responsabile per conto di propri clienti, tra i quali l'Azienda ospedaliera di Perugia, in violazione dell'art. 28, parr. 2 e 4, del Regolamento.

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

- "le violazioni contestate riguardano elementi puramente formali, dal momento che non ci sono stati incidenti che abbiano compromesso integrità, disponibilità e confidenzialità dei dati trattati dagli Ospedali di Perugia […] ISWEB non ha commesso le violazioni contestate […] le violazioni sarebbero di natura meramente formale e, comunque, prive di offensività dal momento che la gestione sostanziale dell'infrastruttura tecnologica risponde a rigorosi criteri di sicurezza quali quelli previsti dall'Agenzia per l'Italia digitale e del Code of Conduct for Cloud Infrastructure Service Providers";

- "la piattaforma di whistleblowing attestata presso Seeweb è accessibile solo tramite IP pubblici degli Ospedali di Perugia che veicolano gli IP interni tramite NAT. […] la configurazione del servizio prevede che gli Ospedali di Perugia raggiungano la piattaforma Whistleblowing tramite i loro tre IP pubblici sui quali convergono in NAT gli IP provati delle strutture. Di conseguenza Seeweb vede passare solo ed esclusivamente l'IP pubblici non associabili alle reti interne. Questi IP sono riferibili a una persona giuridica e dunque il loro trattamento non è regolato dalla normativa sulla protezione dei dati personali. Inoltre, né Seeweb né ISWEB trattano dati ulteriori che, associati ai numeri IP, consentono di identificare o rendere identificabili gli utenti che accedono alla piattaforma di whistleblowing";

- "né Seeweb né ISWEB trattano dati ulteriori che, associati ai numeri IP, consentono di identificare o rendere identificabili gli utenti che accedono alla piattaforma di whistleblowing. Ne consegue che nessuna delle due società sta eseguendo trattamenti di dati personali. La Corte di giustizia UE, infatti, ha affermato che i numeri IP non sono necessariamente dati personali, ma che lo diventano se il titolare può concretamente associarli ad altri dati che rendono identificati o identificabili gli utenti";

- "i numeri IP in questione sono esclusi dalla definizione di dato personale dal momento che non è possibile, anche tramite incrocio con altri dati, identificare o rendere identificabile una persona fisica";

- "anche in considerazione del fatto che l'intero servizio non implica una delega al trattamento di dati personali, ISWEB non doveva stipulare il data processing agreement con Seeweb, non doveva ottenere l'autorizzazione degli Ospedali di Perugia e non avrebbe dovuto informarli della presenza di Seeweb";

- la Società "ha chiaramente descritto la struttura tecnica del servizio agli Ospedali di Perugia indicando la presenza di Seeweb come fornitore dell'infrastruttura cloud prima della conclusione del contratto. Di conseguenza con l'accettazione dell'offerta e l'esecuzione del contratto, gli Ospedali di Perugia hanno autorizzato la modalità di erogazione del servizio in

modalità Saas anche tramite Seeweb";

- "premesso che l'oggetto del contratto con gli Ospedali di Perugia non è il trattamento dei dati delle segnalazioni ma solo la messa a disposizione di una infrastruttura tecnologica, né ISWEB né Seeweb possono prendere cognizione dei dati delle segnalazioni che sono cifrati con chiave esclusivamente a disposizione degli Ospedali di Perugia";

- "l'oggetto del contratto fra ISWEB e gli Ospedali di Perugia non riguarda il trattamento dei dati generati dalla piattaforma Saas ma la messa a disposizione del servizio Whistleblowing secondo le caratteristiche indicate nell'offerta commerciale e negli allegati tecnici. Ne consegue che il trattamento dei numeri IP (che, si ripete, nel caso di specie non sono dati personali e comunque sono assegnati a un ente pubblico) non sono oggetto di trattamento da parte degli Ospedali di Perugia. Come ulteriore conseguenza, anche per questa ragione non era dovuta la stipulazione con Seeweb di un contratto da sub-processor. Inoltre, va considerato che né il GDPR né il Codice dei dati personali prevedono una formalità specifica per informare il titolare del trattamento circa le modalità con le quali vengono erogati i servizi, rilevando piuttosto la conoscenza effettiva di quanto accade. Nel caso specifico, gli Ospedali di Perugia erano consapevoli dell'esistenza di Seeweb e dell'utilizzo delle sue infrastrutture dal momento che la circostanza era ben evidenziata nell'offerta commerciale. Pertanto, gli Ospedali di Perugia erano informati dell'esistenza di Seeweb al momento della stipulazione e, con la stipulazione, hanno autorizzato (ove mai fosse stato necessario) il ricorso al sub-processor. Prova che le informazioni in questione erano a conoscenza degli Ospedali di Perugia è nel documento "Assistenza tecnica" (Allegato 1) parte integrante dell'offerta commerciale. Nello specifico, a pagina 7 è chiarito che L'infrastruttura server network ISWEB e fornita da Seeweb S.r.l..";

- "anche nel caso del rapporto fra ISWEB e Seeweb, l'accordo ex art. 28 GDPR non era necessario. ISWEB, infatti, acquista da Seeweb l'infrastruttura necessaria a far funzionare la piattaforma di whistleblowing, senza delegare né la definizione delle finalità né delle modalità dei trattamenti a Seeweb";

- "Isweb non tratta i dati delle segnalazioni che sono cifrati e nell'esclusiva disponibilità degli Ospedali di Perugia [...] in nessun modo Seeweb può acquisire informazioni sull'acquisizione e la gestione delle condotte illecite dal momento che la connessione con la piattaforma di whistleblowing avviene sempre con lo stesso IP pubblico della struttura interessata e, in ogni caso, non è possibile associare l'IP che si collega alla piattaforma con la segnalazione. Queste circostanze, come anche il funzionamento generale della piattaforma di whistleblowing, erano e sono perfettamente conoscibili dagli Ospedali di Perugia anche in considerazione del fatto che la piattaforma in questione è regolata da una licenza d'uso che consente la libera accessibilità dei codici sorgenti. Di conseguenza, gli Ospedali di Perugia erano e sono in condizioni di conoscere esattamente tutte le caratteristiche necessarie alla propria conformità normativa";

- "nell'ambito della revisione dei propri processi commerciali, ISWEB ha avviato un'attività di ulteriore chiarificazione della modalità di erogazione dei servizi in modalità as a service consistente nella ripetizione delle informazioni sull'utilizzo di Seeweb contenute nella documentazione tecnica anche nell'offerta commerciale e prevedendo un'espressa accettazione della modalità di erogazione del servizio in luogo dell'accettazione tramite stipulazione contrattuale".

In data XX si è, inoltre, svolta l'audizione richiesta dalla Società, ai sensi dell'art. 166, comma 6, del Codice, a seguito della quale la Società ha fornito all'Autorità "copia del messaggio di posta elettronica inviato in data 17 dicembre 2015 all'Azienda ospedaliera di Perugia, al quale era allegato, tra gli altri, il documento tecnico denominato "Server Network ISWEB", dal quale si

evince chiaramente l'infrastruttura utilizzata per l'erogazione del servizio" (cfr. nota del XX e relativi allegati).

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 (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).

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 in materia di protezione dei dati personali (spec. artt. 6, par. 1, lett. c), 9, par. 2, lett. b), 10 e 88, par. 1, del Regolamento).

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).

In tale quadro, il responsabile non può ricorrere a un altro responsabile “senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento” e, in tal caso, “su tale altro responsabile del trattamento sono imposti […] gli stessi obblighi in materia di protezione dei dati, contenuti nel contratto o in altro atto giuridico tra il tritolare del trattamento e il responsabile del trattamento” (art. 28, parr. 2 e 4, del Regolamento).

3.1. I trattamenti effettuati dalla Società per conto dell’Azienda sanitaria di Perugia: mancata regolamentazione del rapporto con il fornitore di servizi di hosting.

Ai fini del rispetto della normativa in materia di protezione dei dati personali occorre identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella del titolare, del responsabile e degli altri responsabili del trattamento, nonché dei soggetti che operano sotto la diretta responsabilità di questi (artt. 4, punti 7) e 8), 24, 28, 29 e 32, par. 4, del Regolamento e art. 2-quaterdecies del Codice).

Nel corso dell’attività ispettiva è emerso che 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” (cfr. all. 7 al verbale del XX).

Sebbene la Società abbia dichiarato che “l’oggetto del contratto con gli Ospedali di Perugia non è il trattamento dei dati delle segnalazioni ma solo la messa a disposizione di una infrastruttura tecnologica” e che “né ISWEB né Seeweb possono prendere cognizione dei dati delle segnalazioni che sono cifrati con chiave esclusivamente a disposizione degli Ospedali di Perugia”, concludendo che “l’intero servizio non implica una delega al trattamento di dati personali” anche in ragione del fatto che “né Seeweb né ISWEB trattano dati ulteriori che, associati ai numeri IP, consentono di identificare o rendere identificabili gli utenti che accedono alla piattaforma di whistleblowing”, deve ritenersi che le operazioni sopra descritte diano comunque luogo a un trattamento di dati personali ai sensi dell’art. 4, punto 2), del Regolamento per i motivi di seguito rappresentati.

Le informazioni presenti all’interno delle segnalazioni di condotte illecite acquisite mediante l’applicativo “whistleblowing” in questione, seppur sottoposti a cifratura – che costituisce 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 – 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).

Come messo in chiarito dal Garante in numerose occasioni, anche tenendo conto degli orientamenti del Comitato europeo di protezione dei dati (cfr. Guidelines 7/2020 on the concepts of controller and processor in the GDPR, adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, in particolare, par. 2.1.4, punto 40, nella parte in cui è riportato l'esempio relativo agli "Hosting services"), il fornitore del servizio di hosting (nel caso di specie, un servizio di hosting di server virtuali o fisici), pur non trattando gli indirizzi IP relativi agli interessati che utilizzano l'applicativo in questione e pur non accedendo direttamente ai dati personali trattati mediante tale applicativo, conserva questi ultimi sulla propria infrastruttura tecnologica e ne garantisce l'integrità e la disponibilità, adottando adeguate misure tecniche e organizzative, assicurando determinati livelli di servizio in termini di disponibilità dei sistemi e mettendo a disposizione dei propri clienti una serie di strumenti per gestire e monitorare il servizio (cfr., con riguardo alla mancata regolazione del rapporto con il fornitore del servizio di hosting, provv. 10 febbraio 2022, n. 44, in corso di pubblicazione, e provv. 11 febbraio 2021, n. 49, doc. web n. 9562852, spec. par. 3.2).

Sul presupposto che i dati trattati dal fornitore del servizio di hosting non costituissero dati personali la Società ha ritenuto di non essere tenuta a "stipulare il data processing agreement con Seeweb" e di non dover "ottenere l'autorizzazione degli Ospedali di Perugia" né di dovere informare il cliente "della presenza di Seeweb".

Dall'esame della documentazione in atti, non risulta infatti essere stato disciplinato il rapporto con Seeweb S.r.l. a cui la Società ha fatto ricorso sia per i trattamenti posti in essere in qualità di titolare (profilo in merito al quale si veda il successivo paragrafo; cfr. art. 28, parr. 1 e 3, del Regolamento), sia per quelli effettuati in qualità di responsabile per conto di propri clienti, tra i quali l'Azienda ospedaliera di Perugia (cfr. art. 28, parr. 2 e 4, del Regolamento).

Nel prendere atto del fatto che il ricorso a Seeweb S.r.l. come fornitore del servizio di hosting fosse stato indicato nella documentazione tecnica messa a disposizione, prima della conclusione del contratto, dell'Azienda ospedaliera di Perugia, la quale quindi non poteva ritenersi del tutto ignara del coinvolgimento di un altro soggetto nel complessivo trattamento, occorre comunque richiamare l'attenzione su quanto previsto dall'art. 28, par. 2, del Regolamento, che richiede espressamente che il responsabile non ricorra a un altro responsabile "senza previa autorizzazione scritta, specifica o generale, del titolare", autorizzazione che, nel caso di specie, non è stata invece acquisita.

Tale previsione è, infatti, funzionale ad assicurare che il titolare del trattamento abbia sempre il pieno controllo dei trattamenti che vengono effettuati per suo conto, potendo, se del caso, opporsi tanto alla possibilità stessa di ricorrere ad "altri responsabili del trattamento", quanto all'individuazione di tali soggetti come effettuata dal "responsabile iniziale" (cfr. art. 28, parr. 2 e 4, del Regolamento).

Sebbene nel corso dell'istruttoria la Società abbia regolamentato in data 18 settembre 2019 il rapporto con Seeweb S.r.l., designandola responsabile del trattamento (cfr. nota del XX), si rileva, tuttavia, che l'atto trasmesso non tiene conto del ruolo di sub-responsabile assunto da Seeweb S.r.l. con riguardo ai trattamenti effettuati per conto dei clienti della Società, ivi incluso quello relativo all'acquisizione e la gestione delle condotte illecite mediante l'applicativo in uso all'Azienda ospedaliera di Perugia.

Per tali ragioni, si ritiene che il ricorso da parte della Società ai servizi offerti da Seeweb S.r.l. – in assenza di un contratto o altro atto giuridico che disciplini il trattamento di dati personali, da parte di quest'ultima, in qualità di sub-responsabile, e senza specifica autorizzazione da parte dell'Azienda in merito al coinvolgimento di tale soggetto – risulta avvenuto in violazione dell'art. 28, parr. 2 e 4, del Regolamento.

3.2. I trattamenti posti in essere dalla società in qualità di titolare del trattamento: mancata

regolamentazione del rapporto con il fornitore di servizi di hosting.

Come evidenziato nel precedente paragrafo, dall'esame della documentazione fornita, risulta che i ruoli assunti con riguardo ai trattamenti di dati personali effettuati dal fornitore di servizi di hosting non fossero stati definiti nel "Contratto generale per la fornitura di servizi Seeweb" o in altri atti giuridici, non essendo disciplinato, ai sensi dell'art. 28, parr. 1 e 3, del Regolamento, il rapporto con Seeweb S.r.l. a cui la Società ha fatto ricorso anche per i numerosi trattamenti posti in essere in qualità di titolare e, dunque, riconducibili a finalità eterogenee (dalla gestione del rapporto di lavoro con i propri dipendenti, alla gestione contabile e amministrativa, ai trattamenti strumentali all'erogazione dei propri servizi) che, per propria natura, possono comportare il trattamento di categorie anche particolari di dati personali e coinvolgere anche interessati "vulnerabili".

Con nota del XX, la Società, ha tuttavia trasmesso copia dell'atto del XX con il quale ha inteso regolamentare il rapporto con Seeweb S.r.l., designandola responsabile del trattamento, limitatamente ai trattamenti svolti per proprio conto.

Al riguardo appare indispensabile ricordare che, 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. 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 (art. 28, par. 3, del Regolamento) e il responsabile del trattamento è quindi, a propria volta, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare" (art. 28, par. 3, lett. a) del Regolamento.

In tali casi la disciplina in materia di protezione dei dati richiede che il rapporto tra il titolare e il fornitore del servizio di hosting 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, in qualità di titolare del trattamento, e il fornitore del servizio di hosting è stato regolato sotto il profilo della protezione dei dati solo a seguito dell'attività ispettiva condotta dal Garante (con riguardo agli specifici rischi derivanti dalla mancata regolamentazione del rapporto, ai sensi dell'art. 28 del Regolamento, con i soggetti che trattano i dati per conto e nell'interesse del titolare del trattamento, provv. 17 settembre 2020, nn. 160 e 161, doc. web nn. 9461168 e 9461321; v. anche provv. 11 febbraio 2021, n. 49, doc. web n. 9562852, provv. 17 dicembre 2020, nn. 280, 281 e 282, doc. web nn. 9524175, 9525315 e 9525337, nonché provv. 10 febbraio 2022, n. 43, doc. web n. 9751498, provv. 10 febbraio 2022, n. 44, in corso di pubblicazione, cit.).

Tanto premesso, tenuto conto delle considerazioni svolte nel precedente paragrafo in merito ai trattamenti svolti dai fornitori dei servizi di hosting e del fatto che, almeno fino al 19 settembre 2019, la Società ha omesso di regolare il trattamento dei dati personali effettuato, per proprio conto e nel proprio esclusivo interesse, da un soggetto esterno (nel caso di specie il fornitore del servizio di hosting), si ritiene che la Società si è resa responsabile della violazione dell'art. 28, parr. 1 e 3, del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal responsabile 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 responsabile del trattamento al fine di attenuare i rischi del trattamento, rispetto alla situazione presente all'atto dell'avvio dell'istruttoria, non consentono tuttavia di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano quindi insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per la determinazione della norma applicabile, sotto il profilo temporale, deve essere richiamato, in particolare, il principio di legalità di cui all'art. 1, comma 2, della l. n. 689/1981, ai sensi del quale le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati. Ciò determina l'obbligo di prendere in considerazione le disposizioni vigenti al momento della commessa violazione, che – data la natura permanente degli illeciti contestati – risulta tuttora in corso. Pertanto, si ritiene che il Regolamento e il Codice costituiscano la normativa alla luce della quale valutare i trattamenti in questione.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato non avendo la Società disciplinato il rapporto con il fornitore del servizio di hosting a cui la Società ha fatto ricorso sia per i trattamenti posti in essere in qualità di titolare, in violazione dell'art. 28, parr. 1 e 3, del Regolamento, sia per quelli effettuati in qualità di responsabile per conto di propri clienti, tra i quali l'Azienda ospedaliera di Perugia, in violazione dell'art. 28, parr. 2 e 4, del Regolamento.

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

5. Misure correttive (art. 58, par. 2, lett. d), del Regolamento).

Considerato che, allo stato, la Società non ha comprovato di aver provveduto a regolamentare il rapporto con il fornitore del servizio di hosting in relazione ai trattamenti effettuati per conto dell'Azienda ospedaliera di Perugia mediante l'applicativo utilizzato per la acquisizione e gestione delle segnalazioni di presunti illeciti, non acquisendo previamente l'autorizzazione del titolare, risulta necessario ingiungere alla Società, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di conformare i trattamenti alle disposizioni in materia di protezione dei dati personali (art. 28, parr. 2 e 4, del Regolamento), entro trenta giorni dalla notifica del presente provvedimento.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, la Società dovrà, inoltre, provvedere a comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese per assicurare la conformità del trattamento al Regolamento.

6. 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).

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

Ai fini dell'applicazione della sanzione, con riguardo ai trattamenti di dati effettuati per conto dell'Azienda ospedaliera di Perugia, 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 al momento delle attività ispettive non erano presenti segnalazioni di condotte illecite all'interno dell'applicativo per l'acquisizione gestione delle segnalazioni di illecito e che nella documentazione fornita in fase precontrattuale all'azienda fosse stato indicato il ricorso ai servizi offerti dalla società Seeweb s.r.l., consentendo con ciò di presumere che l'Azienda fosse quantomeno a conoscenza del coinvolgimento di un altro soggetto nel complessivo trattamento.

Con riguardo ai trattamenti effettuati in qualità di titolare è stato considerato che il servizio di Hosting, affidato senza che fosse previamente disciplinato il ruolo del fornitore ai sensi della disciplina di protezione dei dati, ha riguardato i molteplici trattamenti che la Società effettua in qualità di titolare per finalità differenti (dalla gestione del rapporto di lavoro con i propri dipendenti, alla gestione contabile e amministrativa, ai trattamenti strumentali all'erogazione dei propri servizi) che, per propria natura, possono comportare il trattamento di categorie anche particolari di dati personali e coinvolgere anche interessati "vulnerabili". Di contro è stato considerato che successivamente all'attività ispettiva la Società ha provveduto a disciplinare il predetto rapporto ai sensi dell'art. 28 del Regolamento e che non risultano, precedenti violazioni commesse dalla stessa 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 dell'art. 28 del Regolamento, atteso che, in relazione al caso specifico, la sanzione risulta effettiva, proporzionata e dissuasiva (art. 83, par. 1, del Regolamento).

Tenuto conto della particolare natura dei dati personali oggetto di trattamento e dei connessi rischi per 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 ISWEB S.p.A. per la violazione dell'art. 28 del Regolamento, nei termini di cui in motivazione;

ORDINA

a ISWEB S.p.A., in persona del legale rappresentante pro-tempore, con sede legale in Via Tiburtina Valeria Km. 112,500, 67068 Scurcola Marsicana (AQ), codice fiscale/partita IVA 01722270665, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 4, del Regolamento, di pagare la somma di 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

a ISWEB S.p.A:

a) 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;

b) ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di conformare, nei termini descritti al punto 5 del presente provvedimento, i trattamenti alle disposizioni in materia di protezione dei dati personali (art. 28, parr. 2 e 4, del Regolamento), entro trenta giorni dalla notifica del presente provvedimento;

c) ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, di comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese per assicurare la conformità del trattamento al Regolamento;

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