Ordinanza ingiunzione nei confronti di Servizio Idrico Integrato S.c.p.a. - 6 ottobre 2022 [9817058]

VEDI ANCHE NEWSLETTER DEL 24 OTTOBRE 2022

[doc. web n. 9817058]

Ordinanza ingiunzione nei confronti di Servizio Idrico Integrato S.c.p.a. - 6 ottobre 2022

Registro dei provvedimenti
n. 328 del 6 ottobre 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 n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 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. Introduzione.

Con reclamo del XX, presentato ai sensi dell'art. 77 del Regolamento, un utente dell'azienda

Servizio Idrico Integrato S.c.p.a. (di seguito, l'"Azienda") ha lamentato la circostanza che sul sito web dell'Azienda sarebbe presente "un'area utente […] dove vengono gestiti i contatti e le fatture [in assenza di un] sistema di cifratura (certificato SSL) [, che,] come è noto, è necessario in quanto è presente un'autenticazione e transitano dati personali". Il reclamante, che ha segnalato tale circostanza anche alla Società "per ben due volte tramite PEC in data XX e precedentemente in data XX", senza aver ricevuto risposta, ritiene che sia stato, pertanto, violato l'"articolo 32 del [Regolamento] (Sicurezza del trattamento) in particolare il comma 2".

L'utilizzo di un protocollo di rete non sicuro (quale il protocollo "http") sul sito web in questione è stato accertato dall'Ufficio del Garante con relazione di servizio del XX.

2. L'attività istruttoria.

Con nota del XX (prot. n. XX), l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, 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, avente ad oggetto le presunte violazioni degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento, invitando il predetto titolare 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 l. 24 novembre 1981, n. 689).

Con nota del XX, l'Azienda, per il tramite del proprio avvocato, ha presentato una memoria difensiva, dichiarando, in particolare, che:

> "all'interno del sito vi è […] un'area riservata dedicata solo agli utenti che hanno un contratto di fornitura di servizio con la società che si sono preventivamente registrati all'arca stessa. Una volta che l'utente ha fornito i dati anagrafici necessari e i dati dell'utenza interessata, vengono fornite delle credenziali di accesso costituite da un nome utente ed una password. Con questi codici l'utente in via diretta, riservata ed esclusiva può verificare e monitorare le informazioni che riguardano la fornitura collegata al contratto di utenza e può visualizzare e stampare le bollette emesse, il servizio prestato, le tariffe applicate, la tipologia d'utenza assegnata, nonché comunicare l'autolettura";
>
> "nessun rilievo è stato mosso circa eventuali violazioni di dati personali intervenute a seguito della situazione oggetto di contestazione tali da comportare effettive lesioni all'integrità, alla riservatezza e alla disponibilità dei dati personali trattati attraverso il sito";
>
> "il profilo di sicurezza del sito medesimo è perfettamente adeguato allo standard attuale riconosciuto, essendo oramai [stata] completata la migrazione sotto protocollo "https" (Ayper text transfer protocol over secure socket layer) [in data XX (v. all. A alla memoria)]";
>
> "SII ha immediatamente adeguato il livello di sicurezza del sito. Tra l'altro si osserva che i certificati utilizzati per il passaggio al protocollo "https" sono stati acquistati molto prima della comunicazione del Garante, questo quale indice dell'azione di allineamento che l'azienda intendeva realizzare";
>
> "gli scritti all'area riservata sono in tutto circa 13.000, tra cui oltre 2.000 imprese a fronte di un bacino di utenza rappresentato dagli abitanti dei 32 comuni dove il servizio è erogato che sono quantificabili in oltre 220.000";
>
> "la contestazione è relativa a condotta colposa poiché le circostanze di fatto escludono alcuna consapevolezza e intenzionalità della violazione";
>
> "è stata fatta una analisi degli accessi che ha restituito, con riferimento al periodo oggetto di verifica, un andamento privo di anomalie e tale da far ritenere che non vi siano stati tentativi

o eventi consumati di violazione dati personali […; inoltre] le password di registrazione sono crittografate";

"a seguito di analisi effettuate sulle attività di trattamento dati personali svolte in azienda, SII ha adottato un sistema di misure tecniche e organizzative adeguate alla gestione dei rischi per i diritti e le libertà delle persone fisiche relativi alle attività di trattamento effettuate in azienda";

"i dati personali potenzialmente esposti a violazione non rientrano tra quelli appartenenti a categorie particolari poiché consistono esclusivamente in nome, cognome o ragione sociale, codice fiscale o partita I.V.A., recapito e-mail e telefonico, prospetti di fatturazione, oltre all'identificativo utente SII";

"nessun beneficio finanziario o di altro genere è derivato a SII dalla condotta oggetto di contestazione. Da essa, poi, nessun danno è sorto a carico dell'interessato reclamante o di altri interessati e, con l'intervento di adeguamento descritto, il rischio di danni alle persone fisiche in relazione ai dati che circolano e sono trasportati dal sito www.siiato2.it è stato abbattuto in linea con la probabilità e la gravità del medesimo, con riferimento allo stato dell'arte e dei costi".

In occasione dell'audizione, richiesta ai sensi dell'art. 166, comma 6, del Codice e tenutasi in data XX (verbale prot. n. XX del XX), l'Azienda ha dichiarato, in particolare, che:

"nell'area riservata non ci sono dati relativi a transazioni economiche, non essendo possibile, ad esempio, pagare le bollette online né attivare domiciliazioni bancarie";

"l'azienda agisce, inoltre, in regime di monopolio e, pertanto, il sito web non ha alcuna finalità commerciale o pubblicitaria, essendo solo volto a fornire delle informazioni utili agli utenti";

"l'azienda ha, dunque, prontamente preso atto di quanto rilevato dall'Ufficio del Garante nel corso dell'istruttoria, provvedendo, in particolare, a crittografare tutte le connessioni degli utenti al sito istituzionale e all'area riservata. Anche a seguito dell'adozione di tali misure non sono stati rilevati incidenti di sicurezza in relazione ai dati personali in questione".

3. Esito dell'attività istruttoria.

Ai sensi dell'art. 5, par. 1, lett. f), del Regolamento, il trattamento di dati personali deve essere effettuato in conformità al principio di "integrità e riservatezza", in base al quale i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Sulla base di tale principio, l'art. 32 del Regolamento prevede che il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, debba mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, "la cifratura dei dati personali".

Inoltre, in base al principio di "protezione dei dati fin dalla progettazione", formalizzato dall'art. 25, par. 1, del Regolamento, il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, deve mettere in atto, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, misure tecniche e organizzative

adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati. Il cons. 78 del Regolamento mette in luce una precisa responsabilità del titolare, ossia quella di valutare costantemente se stia utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità esistenti. Inoltre, il titolare dovrebbe effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali.

L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica anche ai sistemi preesistenti. Ciò implica che i sistemi progettati prima dell'entrata in vigore del Regolamento devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in modo efficace (cfr. le "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita" adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020, spec. punti 38 e 84).

Con particolare riferimento al principio di "integrità e riservatezza", il titolare deve (cfr. le citate Linee guida 4/2019 sull'articolo 25, spec. punto 85):

> valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti e le libertà degli interessati, e contrastare efficacemente quelli identificati;
>
> proteggere i dati personali da modifiche e accessi non autorizzati e accidentali durante il loro trasferimento.

Ciò premesso, sulla base degli elementi acquisiti e dei fatti emersi a seguito dell'attività istruttoria, è stato accertato che l'accesso al sito web dell'Azienda dedicato ai "servizi online" (raggiungibile all'indirizzo http://...) avveniva tramite il protocollo di rete "http" (hypertext transfer protocol). È stato, altresì, accertato che la pagina principale del citato sito web conteneva i moduli per l'inserimento delle credenziali di autenticazione (nome utente e password) degli utenti. Inoltre, come emerge dalla documentazione agli atti, all'interno della sezione "Anagrafica" dell'area personale sul sito web in questione sono consultabili dati personali dell'utente, quali il codice cliente, il nome e cognome, il numero di telefono, il codice fiscale, l'eventuale partita IVA, l'indirizzo di posta elettronica, l'indirizzo di residenza e il tipo di servizio erogato. All'interno della sezione "Fatture" è anche possibile visualizzare e scaricare le fatture emesse dalla Società a fronte dei servizi erogati all'utente.

Al riguardo, l'Autorità, anche in vigenza del precedente quadro normativo in materia di protezione dei dati personali, ha affermato che l'interazione di un utente con un sito web ai fini della trasmissione di dati personali debba essere protetta con protocolli crittografici SSL (Secure Socket Layer), garantendo una migliore sicurezza a fronte dei rischi di furto di identità sempre presenti nell'interazione web con normali protocolli http in chiaro (v., tra gli altri, provv.ti 10 giugno 2021, n. 235, doc. web n. 9685922; 2 dicembre 2021, n. 422, doc. web n. 9734884; 2 dicembre 2021, n. 423, doc. web n. 9734934; 27 gennaio 2022, n. 34, doc. web n. 9746448; 24 marzo 2022, n. 107, doc. web n. 9767635; 26 maggio 2022, n. 201, doc. web n. 9790365).

L'utilizzo di tecniche crittografiche, allo stato dell'arte, è, infatti, una delle misure comunemente adottate per proteggere, in particolar modo, le credenziali di autenticazione degli utenti di un servizio online durante la loro trasmissione su rete internet; ciò tenuto conto degli elevati rischi presentati dal trattamento di tali dati, che possono derivare dall'accesso non autorizzato agli stessi o dalla loro divulgazione, anche in ragione dell'abitudine di molti utenti a riutilizzare la stessa password, o comunque una password molto simile, per l'accesso a diversi servizi online.

L'accesso al sito web in questione avveniva, invece, in modo non sicuro, mediante il protocollo di

rete “http” (hypertext transfer protocol). Tale protocollo non garantiva, infatti, la riservatezza e l’integrità dei dati scambiati tra il browser dell’utente e il server che ospita il sito web dell’Azienda, e non consentiva agli utenti di verificare l’autenticità del sito web visualizzato. Tenuto conto della natura, dell’oggetto e della finalità del trattamento, nonché dei rischi che insistono sui dati, tra cui il rischio di furto di identità, di possibile clonazione del sito web a scopo di phishing e di acquisizione delle credenziali di autenticazione per fini illeciti, la soluzione adottata dall’Azienda non poteva, pertanto, essere considerata una misura tecnica idonea a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento.

Il mancato utilizzo di tecniche crittografiche per il trasporto dei dati configura una violazione dell’art. 5, par. 1, lett. f), e dell’art. 32 del Regolamento, il cui par. 1, lett. a), individua, peraltro, espressamente la cifratura dei dati come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio (sul punto, cfr. anche il considerando n. 83 del Regolamento nella parte in cui prevede che “il titolare del trattamento […] dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura”).

La Società avrebbe dovuto mettere in atto, fin dalla progettazione del proprio sito web, misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, tra cui il principio di “integrità e riservatezza”, provvedendo ad adottare un protocollo di rete sicuro, quale il protocollo “https” (hypertext transfer protocol over secure socket layer), nell’ambito del sito web oggetto del reclamo. Pertanto, il trattamento in esame è avvenuto, altresì, in violazione dell’art. 25, par. 1, del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell’istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell’art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall’Ufficio con l’atto di avvio del procedimento e risultano insufficienti a consentire l’archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall’art. 11 del Regolamento del Garante n. 1/2019.

Si rappresenta, altresì, che 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 che sancisce come «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 dell’illecito contestato – deve essere individuato all’atto di cessazione della condotta illecita, verificatasi successivamente alla data del 25 maggio 2018 in cui il Regolamento è divenuto applicabile e il d.lgs. 10 agosto 2018, n. 101 è entrato in vigore. Dagli atti dell’istruttoria è, infatti, emerso che l’Azienda ha adottato il protocollo “https” in data XX.

Si confermano, pertanto, le valutazioni preliminari dell’Ufficio e si rileva l’illiceità del trattamento di dati personali effettuato dall’Azienda per non aver messo in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, in violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento, nonché per aver omesso di mettere in atto, fin dalla progettazione del sito web, misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, in violazione dell’art. 25, par. 1, del Regolamento.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall’art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, atteso che l'Azienda ha adottato il protocollo "https" in data XX, non ricorrono i presupposti per l'adozione di ulteriori 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 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.

In relazione ai predetti elementi è stato tenuto conto dell'alto numero di interessati, iscritti all'area riservata del sito web dell'Azienda, i cui dati personali sono oggetto di trattamento ("in tutto circa 13.000, tra cui oltre 2.000 imprese"). È, stato, inoltre considerato che, sebbene il reclamante avesse fatto presente in due occasioni all'Azienda l'insufficienza delle misure di sicurezza adottate sul predetto sito, l'Azienda non si è prontamente attivata, prima dell'avvio dell'istruttoria da parte del Garante, per porre fine alla violazione.

Di contro, si è tenuto in considerazione che l'Azienda, una volta appreso del procedimento avviato dall'Autorità, ha tempestivamente adottato le necessarie misure volte a risolvere la criticità di sicurezza sul proprio sito web, prestando piena collaborazione nel corso dell'istruttoria. Non risultano, infine, precedenti violazioni pertinenti 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 15.000 (quindicimila) per la violazione degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto dell'alto numero di interessati iscritti all'area riservata del sito web dell'Azienda, i cui dati sono oggetto di trattamento, 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 art. 16 del Regolamento del Garante n. 1/2019.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dal Servizio Idrico Integrato S.c.p.a. per violazione degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento, nei termini di cui in motivazione;

ORDINA

al Servizio Idrico Integrato S.c.p.a., in persona del legale rappresentante pro-tempore, con sede legale in Via I Maggio, 65 - 05100 Terni (TR), C.F. 01250250550, di pagare la somma di euro 15.000 (quindicimila) 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 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Azienda, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di 15.000 (quindicimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione del presente provvedimento sul sito web del Garante, ritenendo che ricorrano i presupposti di cui all'art. 17 del Regolamento del Garante n. 1/2019.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, 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, 6 ottobre 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei