Ordinanza ingiunzione nei confronti di Azienda sanitaria locale di Bari - 28 giugno 2018 [9039235]

[doc. web n. 9039235]

Ordinanza ingiunzione nei confronti di Azienda sanitaria locale di Bari - 28 giugno 2018

Registro dei provvedimenti
n. 399 del 28 giugno 2018

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO l'art. 1, comma 2, della legge 24 novembre 1981, n. 689, ai sensi del quale le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e per i tempi in esse considerati;

RILEVATO che la Guardia di finanza, Nucleo speciale privacy, con verbale n. 5 del 18 gennaio 2018 (notificato l'8 febbraio 2018), che qui deve intendersi integralmente riportato, ha contestato all'Azienda sanitaria locale (di seguito Asl) di Bari, in persona del legale rappresentante pro-tempore, con sede legale in Bari, lungomare Starita n. 6, C.F. 06534340721, la violazione delle disposizioni di cui agli artt. 33 e 162, comma 2-bis, del Codice in materia di protezione dei dati personali (d. lg. 30 giugno 2003, n. 196, di seguito denominato "Codice");

RILEVATO che dall'esame degli atti del procedimento sanzionatorio avviato con la contestazione di violazione amministrativa è emerso, in sintesi, quanto segue:

- la Guardia di finanza ha svolto un accertamento ispettivo nei confronti dell'Asl di Bari, presso il presidio ospedaliero San Giacomo di Monopoli, nei giorni 21, 22 e 23 novembre 2017, nell'ambito del programma semestrale di ispezioni stabilito dal Garante;

- nel corso dell'accertamento, durante il quale sono stati esaminati i diversi applicativi informatici in uso presso il presidio, è emerso che le credenziali per l'accesso ad alcuni di essi (Hdgold Olivetti, Hospital Cardio, Geos, Gepadial, Armonia, Emodata) sono condivise fra i dipendenti che li utilizzano. E' inoltre emerso che, con riferimento a due sistemi (Hospital Cardio e Edotto Sist), alcuni dipendenti vi accedono utilizzando password composte da meno di otto caratteri alfanumerici;

- sulla base dei predetti elementi, la Guardia di finanza ha redatto il verbale di contestazione di violazione amministrativa n. 5 del 18 gennaio 2018;

RILEVATO che con il citato verbale è stata contestata all'Asl di Bari, ai sensi dell'art. 162, comma 2-bis, del Codice, la violazione degli artt. 33 e ss. del Codice e delle regole del disciplinare tecnico di cui al relativo allegato B);

LETTI gli scritti difensivi del 5 marzo 2018, ove si osserva, in sintesi, quanto segue:

- "con riferimento al sopralluogo effettuato dal Nucleo Speciale Privacy presso il Presidio Ospedaliero San Giacomo di Monopoli, sono stati sottoposti a controllo alcune postazioni di lavoro non collegate (c.d. join) al dominio unico aziendale. Tale circostanza si configura come caso eccezionale in considerazione della politica di sicurezza generale definita

dall'azienda per la quale tutte le postazioni di lavoro devono essere sottoposte alle misure minime di sicurezza, come disciplinato dagli artt. 33-34 del Codice in materia di protezione dei dati personali. Si evidenzia che già dall'anno 2011 l'ASL di Bari ha provveduto all'adozione di un Regolamento interno per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche aziendali […]. Con riferimento al rilievo di condivisioni di password tra operatori, si precisa che l'ASL di Bari ha sempre disciplinato e sensibilizzato tutto il personale aziendale sulle tematiche della protezione e riservatezza dei dati personali. Il Regolamento di cui sopra al capitolo n. 4 par. 4.2 dispone che le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'U.O.A.S.S.I. [Unità operativa analisi del sistema informatico], associato ad una parola chiave (password) riservata e creata dall'incaricato che dovrà essere memorizzata, custodita con la massima diligenza e non divulgata. Si evidenzia, inoltre, che l'Azienda non ha implementato un Single Sign On per cui anche l'accesso al dominio non consente di utilizzare i sistemi applicativi, che gestiscono dati personali e/o sensibili, se non dopo una specifica autenticazione applicativa che prevede credenziali nominative con abilitazioni diversificate per tipologia di utente così come certificato dai fornitori di software applicativo.";

- "le omissioni rilevate e contestate dal Nucleo Speciale Privacy sono state determinate da comportamenti di soggetti autorizzati dell'ASL di Bari in violazione del Regolamento interno aziendale, adottato con deliberazione del Direttore Generale n. 925 del 16 maggio 2011, rilevando in tal senso l'esclusione di responsabilità del Titolare del trattamento, incolpevole nel caso di specie e sempre attento all'osservanza della disciplina in materia di protezione dei dati personali, con la sempre dimostrata ordinaria diligenza".

RITENUTO che le argomentazioni addotte non risultano idonee a determinare l'archiviazione del procedimento sanzionatorio avviato con la contestazione di cui sopra per le ragioni di seguito esposte:

- emerge, dai verbali di operazioni compiute nel corso dell'accertamento ispettivo presso il presidio San Giacomo di Monopoli, la cui organizzazione in materia di sicurezza nei trattamenti di dati personali ricade sotto la responsabilità dell'Asl di Bari in quanto titolare dei trattamenti medesimi, una non episodica violazione delle regole sull'autenticazione informatica dettate dagli artt. 33 e ss. del Codice e dalle regole nn. 3, 4, 5 e 6 del disciplinare tecnico di cui all'allegato B) del Codice medesimo;

- tale violazione, per il suo carattere di sistematicità, deve attribuirsi alla responsabilità dell'Asl di Bari, la quale non ha adottato idonei accorgimenti per impedire che gli accessi ai sistemi avvenissero con l'utilizzo di password composte da un numero di caratteri alfanumerici inferiori a otto e con la condivisione delle credenziali di autenticazione fra più incaricati del trattamento;

RILEVATO, quindi, che l'Asl di Bari, sulla base delle considerazioni sopra richiamate, risulta aver commesso la violazione prevista dall'art. 162, comma 2-bis, del Codice, per aver omesso di adottare le misure minime di sicurezza previste dagli artt. 33 e ss. del Codice e dalle regole nn. 3, 4, 5 e 6 del disciplinare tecnico di cui all'allegato B) del medesimo Codice;

VISTO l'art. 162, comma 2-bis, del Codice, che punisce la violazione degli artt. 33 e ss. e delle regole dettate dal disciplinare tecnico di cui all'allegato B) del Codice, con la sanzione amministrativa del pagamento di una somma da 10.000 a 120.000 euro;

CONSIDERATO che, ai fini della determinazione dell'ammontare della sanzione pecuniaria, occorre tenere conto, ai sensi dell'art. 11 della legge n. 689/1981, dell'opera svolta dall'agente per eliminare o attenuare le conseguenze della violazione, della gravità della violazione, della personalità e delle condizioni economiche del contravventore;

CONSIDERATO che, nel caso in esame:

a) in ordine all'aspetto della gravità con riferimento agli elementi dell'entità del pregiudizio o del pericolo e dell'intensità dell'elemento psicologico, la violazione non risulta connotata da elementi specifici;

b) ai fini della valutazione dell'opera svolta dall'agente, deve essere considerato in termini non favorevoli il fatto che l'Asl non abbia comunicato al Garante eventuali provvedimenti adottati a seguito della contestazione di violazione amministrativa al fine di adeguare le misure di sicurezza alle vigenti disposizioni normative;

c) circa la personalità dell'autore della violazione, l'Asl risulta gravata da un precedente procedimento sanzionatorio specifico in materia di misure minime di sicurezza definito con ordinanza-ingiunzione (provvedimento n. 7 del 10 gennaio

2013);

d) in merito alle condizioni economiche dell'agente, è stato preso in considerazione il bilancio per l'anno 2017;

RITENUTO, quindi, di dover determinare, ai sensi dell'art. 11 della L. n. 689/1981, l'ammontare della sanzione pecuniaria, in ragione dei suddetti elementi valutati nel loro complesso, nella misura di euro 20.000 (ventimila);

VISTA la documentazione in atti;

VISTA la legge n. 689/1981, e successive modificazioni e integrazioni;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000, adottato con deliberazione del 28 giugno 2000;

RELATORE la prof.ssa Licia Califano;

ORDINA

all'Azienda sanitaria locale di Bari, in persona del legale rappresentante pro-tempore, con sede legale in Bari, lungomare Starita n. 6, C.F. 06534340721, di pagare la somma di euro 20.000 (ventimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione;

INGIUNGE

alla medesima Azienda sanitaria di pagare la somma di euro 20.000 (ventimila), 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 legge 24 novembre 1981, n. 689.

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 28 giugno 2018

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia