La diffusione accidentale di dati personali trattati da una piattaforma on line costituisce trattamento illecito

Autore: Muia' Pier Paolo
In: Giurisprudenza commentata

Garante per la protezione dei dati personali: Provvedimento n. 17 del 23 gennaio 2020

Fatto

L' Università degli studi "La Sapienza" di Roma ha comunicato al Garante della privacy, secondo quanto imposto dal GDPR, che erano stati dispersi i dati personali comuni di due soggetti, dalla piattaforma internet utilizzata dall' ateneo per le segnalazioni ai sensi della normativa in materia di whistleblowing.

In particolare, l' Università faceva presente al Garante che si era dotata di una piattaforma internet all'interno della quale i dipendenti dell' Ateneo e i soggetti terzi potevano effettuare le segnalazioni di condotte illecite perpetrate dai dipendenti (c.d. whistleblowing) e che si era verificata la dispersione del nome e cognome, indirizzo della sede, indirizzo email e data della segnalazione di un dipendente dell' Ateneo e di una studentessa, in considerazione del fatto che era stato pubblicato sul sito web l' elenco dei segnalanti e le relative pagine web erano state indicizzate dai motori di ricerca.

L' Università appena era venuta a conoscenza della situazione, aveva provveduto a comunicare la dispersione dei dati al Garante entro il termine di 72 ore previsto dal GDPR nonché a bloccare l'accesso alla piattaforma internet e a comunicare la perdita dei dati anche ai diretti interessati.

Dopo di che l'Ateneo aveva sospeso la piattaforma nonché fatto cancellare dai motori di ricerca le copie di cache delle pagine web che riportavano i dati personali e ottenuto la rimozione completa dai risultati di ricerca dai motori google e bing.

Volume consigliato

Diritto & Diritti ISSN 1127-8579

La decisione del Garante

A seguito della comunicazione effettuata dall' Università, il Garante privacy ha notificato all' Ateneo – quale titolare del trattamento – l' avvio del procedimento per verificare le violazioni e applicare le eventuali sanzioni previste dal GDPR.

In particolare, il Garante ha ritenuto che nel caso di specie si fosse verificato un trattamento illecito di dati personali in quanto:

- non rispetta i principi di "liceità, correttezza e trasparenza";
- manca un idoneo presupposto normativo;
- viola le norme in materia di protezione dei dati personali dei dipendenti;
- non sono state adottate misure tecniche e organizzative volte a garantire la riservatezza e la integrità dei dati trattati attraverso la piattaforma on line

L' Università ha replicato agli addebiti mossi dal Garante evidenziando, preliminarmente, come la violazione si sarebbe verificata in un momento precedente alla applicabilità del GDPR e pertanto non potrebbero essergli contestate violazioni di principi previsti da tale normativa e comunque come la mancanza dell' idoneo presupposto normativo non sarebbe applicabile in questo caso in quanto si tratta di un data breach accidentale e non di un trattamento dati volontario. Rispetto ai dati del lavoratore, poi, ha evidenziato che la normativa riguarderebbe soltanto la mancata adozione di misure tecniche e organizzative e pertanto tale fattispecie non sarebbe ravvisabile nel caso oggetto di esame. Infine, l' Ateneo ha rilevato che la causa che ha generato la perdita dei dati è connessa ad un aggiornamento obbligatorio del software di gestione della piattaforma sul quale lo stesso Ateneo non poteva avere alcun controllo e che comunque le pagine contenenti i dati di cui è causa era individuabile tramite i motori di ricerca soltanto inserendo come parole chiavi il nome del segnalante o la data della segnalazione (e pertanto soltanto il segnalante stesso, o al massimo il Responsabile della Prevenzione della Corruzione e della Trasparenza, potevano conoscere tali elementi necessari per trovare le pagine).

Il Garante privacy ha rigettato le argomentazioni difensive proposte dall'Università, rilevando, in primo luogo, che – **in base al principio per cui si devono applicare le disposizioni vigenti al momento in cui è stato commesso il fatto – al caso in esame si applica il GDPR, in quanto trattasi di fattispecie di illecito permanente che si è perfezionata soltanto nel momento in cui i dati personali illecitamente divulgati sono stati rimossi dalle pagine web e cioè dopo il dicembre 2018** (dopo che l' Università aveva avuto conoscenza della dispersione). Pertanto, la fattispecie si è

Diritto & Diritti ISSN 1127-8579

perfezionata dopo che il GDPR era diventato applicabile.

Ciò detto, il Garante ha confermato la illeicità del trattamento per violazione delle disposizioni in materia di sicurezza dei dati.

Il GDPR, infatti, prevede che il titolare del trattamento debba adottare delle misure tecniche e organizzative adeguate a proteggere i dati personali da trattamenti non autorizzati o illeciti ma anche dalla loro perdita o distruzione accidentali. Inoltre, **le misure tecniche e organizzative debbono essere individuate valutando il rischio che nel caso concreto hanno i dati oggetto del trattamento di essere divulgati senza autorizzazione**.

Ebbene, il Garante ha ritenuto che, nel caso di specie, il software utilizzato dall' Università per il whistleblowing era stato installato dal fornitore che ne aveva implementato le componenti senza permettere all' Ateneo di poterlo personalizzare in base alle sue esigenze e valutazioni.

Inoltre, il Garante ha potuto verificare che **i dati identificativi dei segnalanti contenuti nella piattaforma in questione erano indicizzabili e rintracciabili senza alcuna limitazione attraverso i normali motori di ricerca e pertanto chiunque avrebbe potuto prendere visione degli stessi con una semplice ricerca su internet. Ciò significa, secondo il Garante, che l' Università non aveva adottato alcuna misura tecnica in grado di limitare l'accesso ai dati ai soli soggetti che erano legittimati a trattarli** (per es. attraverso credenziali di autenticazione e specifici profili di autorizzazione).

È evidente, quindi, la violazione del principio di sicurezza dei dati sopra esposto.

Tale violazione è riscontrabile anche se, come sostenuto dall' Università, la perdita accidentale dei dati è dipesa da un aggiornamento obbligatorio del software (rispetto al quale, quindi, il titolare del trattamento non poteva fare niente), in quanto **sul titolare grava comunque l'obbligo di testare e verificare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza dei dati oggetto di trattamento**.

Il Garante ha, inoltre, ritenuto che l' Ateneo avesse violato il principio di sicurezza dei dati anche rispetto al trasporto e alla conservazione dei dati. Infatti, dall' istruttoria è emerso che l'indirizzo web attraverso il quale si poteva accedere all' applicativo whistleblowing dell' Università non era crittografato (cioè non usava un protocollo "https:", ma era un semplice protocollo "http:"). Ebbene, il protocollo "http:" non garantisce una comunicazione sicura, sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato.

Pertanto, **posto che il principio di sicurezza dei dati di cui al GDPR prevede anche che il titolare del trattamento utilizzi tecniche di cifratura dei dati fra le misure di sicurezza tecniche che deve adottare per garantire la sicurezza dei dati, il mancato utilizzo da parte dell' Università del**

Diritto & Diritti ISSN 1127-8579

protocollo cifrato (“https:”) per il trasporto dei dati sostanzia una violazione del suddetto principio.

In considerazione delle accertate suddette violazioni della disciplina in materia di protezione dei dati personali, il Garante ha comminato all’ Università la sanziona amministrativa pecuniaria dell’ importo di Euro 30.000, valutata tenuto conto – da un lato - della particolare gravità della condotta posta in essere dall’ Ateneo e della intensità dell’ elemento soggettivo (trattandosi, secondo il Garante, di una grave negligenza del titolare), posto che non era stato adottato alcun accorgimento a tutela della sicurezza dei dati nonché – dall’altro lato – il numero esiguo degli interessati coinvolti (soltanto due) e delle misure adottate per eliminare le cause della violazione (cioè l’ aver provveduto, l’ Ateneo, immediatamente dopo essere venuto a conoscenza della dispersione, a far deindicizzare le pagine web).

Il Garante, invece, non ha adottato alcuna misura correttiva, in considerazione del fatto che la condotta illecita aveva esaurito i suoi effetti e l’ Ateneo aveva provveduto a sospendere l’ applicativo in questione.

Volume consigliato

https://www.diritto.it/la-diffusione-accidentale-di-dati-personali-trattati-da-una-piattaforma-on-line-costituisce-trattamento-illecito/

Diritto & Diritti ISSN 1127-8579