Tecniche di strong authentication richieste dalla normativa privacy sono rivolte a tutte le aziende indipendentemente dalla loro dimensione

Autore: Muia' Pier Paolo
In: Diritto civile e commerciale, Focus

Garante per la protezione dei dati personali: provvedimento n.429 del 19 Luglio 2018

Riferimenti normativi: artt. 17, 132 del Codice in materia di protezione dei dati personali; Cass. Civ. Sez. lav. 12 luglio 2010, n. 16320

Fatto

Il nucleo speciale privacy della Guardia di Finanza aveva svolto degli accertamenti nei confronti di una Società operante nel campo dell'erogazione di servizi di accesso ad internet al fine di accertare il rispetto della normativa in materia di protezione dei dati personali.
In particolare la Guardia di finanza nel corso degli **accertamenti** aveva avuto modo di appurare che la Società nel trattare i dati di traffico telematico per finalità di accertamento e repressione dei reati aveva provveduto a conservarli oltre il termine di 12 mesi, in violazione di quanto disposto dalla normativa in materia di privacy, omettendo, altresì, di adottare la procedura di strong authentication con riferimento all'utilizzo della tecnologia basata sull'elaborazione di caratteristiche biometriche dell'interessato.
La Società di fronte a tali contestazioni aveva reso le proprie giustificazioni, sostenendo di aver adottato misure più che adeguate a garantire la sicurezza e protezione dei dati personali dei propri clienti, avendo predisposto sistemi di autenticazione basati sull'inserimento di **user id e password a**ssegnate ad ogni incaricato dell'azienda. La Società, aveva poi espresso la propria difficoltà a dotarsi di sistemi di riconoscimento biometrico, come il riconoscimento della retina e papillare, a causa delle dimensioni dell'azienda, oltretutto era stato evidenziato dall'azienda l'inopportunità dell'adozione di tali sistemi visti non solo l'esiguità del personale preposto all'accesso dei dati di traffico telematico, ma anche delle misure di sicurezza già adottate (password e user id).
In riferimento ai tempi di conservazione, e dunque alla conservazione di un periodo eccedente i 12 mesi, la Società si era scusata appellandosi ad un errore nell'interpretazione della normativa di riferimento.

Diritto & Diritti ISSN 1127-8579

La decisione del Garante

Il Garante, valutate le dichiarazioni della Società, ha confermato le contestazioni mosse dalla Guardia di Finanza, riconoscendo nel trattamento dei dati personali operato dalla stessa un trattamento illecito, avendo essa conservato i dati di traffico telematico per finalità di accertamento e repressione dei reati per un periodo superiore a 12 mesi nonché per aver essa mancato di adottare le misure prescritte dal Garante e riferite alla **procedura di strong authentication.**
In particolare il Garante, in riferimento alla conservazione dei dati per finalità di accertamento e repressione dei reati, richiamando precedenti provvedimenti, ha ricordato che nell'ambito delle tecniche di strong authentication una di tale tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento. E tali prescrizioni – ha evidenziato il Garante – sono rivolte a tutti gli operatori del settore a prescindere dalle loro capacità organizzative ed economiche o dalla quantità di dati trattati. Ciò di cui si deve tenere conto è la natura particolarmente delicata dei dati oggetto del trattamento e delle finalità perseguite. Secondo il giudizio del Garante nel caso di specie le misure di sicurezza che la Società aveva adottato, e consistenti nell'assegnazione di un user id e di una password, nonché nell'utilizzo di una chiave crittografata, non possono essere considerati rispondenti alle tutele richieste dalla normativa in materia, non essendo idonee a garantire la tutela dei diritti e delle libertà degli interessati.
Con riguardo ai tempi di conservazione dei dati di traffico telematico, ed in particolare alle giustificazioni rese dalla Società, vale a dire l'errata interpretazione della normativa, il Garante precisa che l'errore sulla liceità della condotta può rilevare in termini di esclusione di responsabilità solo quando risulti che questo sia inevitabile ed incolpevole. Per essere considerato tale – ha spiegato il Garante – vi deve essere un elemento positivo, estraneo all'autore della violazione, tale da indurre a pensare che il suo agito sia lecito, nonché a pensare che da parte dell'autore sia stato fatto tutto il possibile per osservare la legge e che, dunque, nessun rimprovero può essergli mosso. Nel caso di specie il Garante ha evidenziato come tali aspetti non sono emersi, tenendo conto anche della posizione della Società, professionalmente inserita in uno specifico campo di attività, e come tale tenuta ad u**n obbligo di informazione e conoscenza più specifico in ordine alle norme che disciplinano il proprio settore di attività**.

Volume consigliato

https://www.diritto.it/tecniche-strong-authentication-richieste-dalla-normativa-privacy-rivolte-tutte-le-aziende-indipendentemente-dalla-dimensione/

Diritto & Diritti ISSN 1127-8579