2013: Il Garante privacy inglese inizia l'anno nuovo con consistenti sanzioni per la Sony

Autore: Marcoccio Gloria
In: Diritto civile e commerciale

L'Information Commissioner Officer -ICO- equivalente inglese della autorità italiana Garante per la protezione dei dati personali, il 14 Gennaio 2013 ha disposto per la Sony (Sony Computer Entertainment Europe Limited) una multa di 250.000 sterline (circa 350.000 euro) per le violazioni di dati personali di un numero assai elevato di utenti della piattaforma Sony PlayStation, avvenute nel corso dell'aprile 2011.

L'autorità inglese ha disposto questa misura nei confronti della Sony in base a quanto stabilito dal "Criminal Justice and Immigration Act" entrato in vigore ad Aprile 2010, che consente all'ICO di definire una multa fino a 500.000 sterline in caso di seria violazione della prescrizione del "Data Protection Act 1998" che impone ad un Titolare di trattamento dati personali l'obbligo di operare in conformità a tale normativa.

L'ICO ha stabilito una multa di consistente valore nei riguardi della Sony per non aver predisposto adeguate misure di sicurezza tecnico-organizzative contro il rischio di accessi non autorizzati e trattamenti illeciti. Come riportato nel Monetary Penalty Notice indirizzato alla Sony[1], l'evento di violazione è risultato causato da diversi attacchi del tipo DDoS (Distribuited Denial of Services) rivolti verso la piattaforma PlayStation in rete (Network Platform) che nel loro complesso hanno comportato l'accesso a nomi, relativi recapiti ed indirizzi email, date di nascita nonché password: dati forniti dai clienti per aprire un account di accesso alla Network Platform.

Nella sua decisione l'ICO ha tenuto conto di molteplici aspetti tra i quali:

Diritto & Diritti ISSN 1127-8579

- l'elevata numerosità dei soggetti interessati (l'ICO riporta stime di utenti PlayStation in termini di milioni, di cui una consistente quota parte in UK);

- mancati aggiornamenti tecnici a cura del Titolare (all'ICO risulta che siano state sfruttate vulnerabilità presenti a causa di mancati aggiornamenti software)

- la criticità della violazione, considerata tale dall'ICO a causa dell'inadeguatezza delle misure in essere rispetto ai rischi specifici esistenti (esplicitamente citata la necessità di misure di sicurezza quali la cifratura delle password)

- la disponibilità da parte del Titolare di ben sufficienti risorse (tecnico-economiche) per poter far fronte a problematiche di sicurezza

- il fatto che il Titolare abbia volontariamente comunicato all'ICO l'evento di violazione dei dati personali, informato i soggetti interessati e offerto loro una forma di riparazione, pienamente cooperato con l'ICO e, a seguito dell'evento di violazione, abbia provveduto ad attuare consistenti misure di protezione (la Network Platform profondamente rivista, aggiunte sofisticate misure di sicurezza, password appropriatamente protette, software riconfigurato,..)

Diritto & Diritti ISSN 1127-8579

Il caso della Sony ha suscitato e continuerà senz'altro a suscitare interesse sotto molteplici punti di vista, considerando anche che contro la decisione dell'autorità inglese la Sony potrà comunque proporre ricorso (per il quale ha tempo fino al 13 Febbraio).

In questa sede l'attenzione è ristretta alla motivazione della sanzione in quanto riguarda, con riferimento alla Network Platform del Titolare, la mancata predisposizione di misure di sicurezza adeguate al profilo di rischio esistente[2] e l'eccesso di dati conservati rispetto a quanto necessario [3].

Volendo rileggere i fatti inglesi dal punto di vista della normativa italiana in materia di protezione dati personali e privacy (D.Lgs 196/03), occorrerebbe senz'altro tenere presenti, come equivalenti non conformità contestabili per l'avvenuto evento di violazione dei dati personali, le prescrizioni di cui all'art.31 "Obblighi di sicurezza" [4] e alla lettera d) del comma 1 dell'art.11 "Modalità del trattamento e requisiti dei dati "[5] insieme all'art. 3 "Principio di necessità nel trattamento dei dati"[6]

Questi requisiti pongono oggettivamente non pochi problemi ad un Titolare chiamato ad osservare la normativa italiana riguardo la predisposizione di misure di sicurezza commensurate a rischi specifici.

Infatti da una parte è evidente la discrezionalità comunque esistente nel decidere quando una misura è sufficiente o meno per contrastare un determinato rischio[7], dall'altra la normativa privacy italiana non fornisce un diretto appiglio per bilanciare queste decisioni tenendo conto dei costi sostenibili (di importanza capitale per la reale implementazione di misure di sicurezza e conseguente reale tutela per i soggetti interessati...), che invece è ben evidente nella norma di origine dell'art.31, ossia la direttiva europea sulla privacy [8].

Diritto & Diritti ISSN 1127-8579

Medesime considerazioni si potrebbero estendere anche per quanto concerne la proporzionalità/necessità dei dati rispetto alle finalità da conseguire (e quindi le conseguenti valutazioni sugli "eccessi" di dati personali trattati).

In caso di non conformità rispetto a queste prescrizioni, il D.Lgs 196/03 non contempla dirette e specifiche sanzioni (come invece è ad esempio il caso delle violazioni delle misure minime di sicurezza, trattate come illecito penale e per le quali sono anche previste consistenti sanzioni amministrative).

Occorre però ricordare che in presenza di tali non conformità si concretizzerebbe una violazione della disciplina rilevante in materia di trattamento dei dati personali (comma 2 art. 11 D.Lgs 196/03, vedasi precedente nota 5) ed in tali circostanze è previsto, da parte del Garante privacy italiano, il divieto e la disposizione del blocco, in tutto o in parte, dei trattamenti e l'adozione di altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali, tra questi la sanzione amministrativa fino a 180.000 euro in caso di non osservanza dei divieto o del blocco di trattamento o delle misure specifiche che il Garante ha facoltà di prescrivere (art. 162 "Altre fattispecie"). Queste sanzioni possono essere anche quadruplicate se considerate inefficaci in ragione della condizione economica del contravventore (art. 164-bis "Casi di minore gravità ed ipotesi aggravate").

Da notare poi che per una tale violazione di dati personali in Italia non sussistono, ad oggi, obblighi di comunicazione verso il Garante privacy e/o verso gli interessati: infatti le recenti variazioni apportate dal D.Lgs 69/12 con il nuovo art. 32.bis "Adempimenti conseguenti ad una violazione di dati personali" introdotto nel D.Lgs 196/03 riguardano esclusivamente i fornitori di servizi di comunicazione elettronica accessibili al pubblico (operatori TLC ed internet provider)[9].

1 http://www.ico.gov.uk/news/latest_news/2013/ico-news-release-2013.aspx

Diritto & Diritti ISSN 1127-8579

2 Principio n. 7 in Part 1 di Schedule 1 e Paragrafo n. 9 in Part 2 di Schedule 1 del “Data Protection Act 1998”

3 Principio n. 3 in Part 1 di Schedule 1 del “Data Protection Act 1998”

4 Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Questa prescrizione deriva dall’art. 17 della direttiva EU sulla privacy 95/46/EU

5 Art. 11. Modalità del trattamento e requisiti dei dati
1. I dati personali oggetto di trattamento sono:

….

Diritto & Diritti ISSN 1127-8579

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Questa prescrizione deriva dalla lettera c comma 1 art. 6 della direttiva EU sulla privacy 95/46/EU.

6Art. 3. Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

7Comunque, una serie di standard internazionali possono fornire una base per tali decisioni (ISO/IEC 27001, COBIT, ...)

8Dal para. 1 dell'art. 17 della direttiva 95/46/EU "...Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

Diritto & Diritti ISSN 1127-8579

9Vedasi anche sull'argomento "Cookies e dintorni: alcune note sul D.Lgs 69/12, recepimento italiano della direttiva europea in materia di privacy nel settore dei servizi di comunicazioni elettroniche accessibili al pubblico" https://www.diritto.it/docs/33576

https://www.diritto.it/2013-il-garante-privacy-inglese-inizia-l-anno-nuovo-con-consistenti-sanzioni-per-la-sony/

Diritto & Diritti ISSN 1127-8579