PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4729 di Martedì 30 giugno 2020

La relazione annuale del Garante per la protezione dei dati personali

Anche quest'anno l'autorità Garante ha presentato la sua relazione annuale. Oltre 200 pagine particolarmente interessanti perché prendono in esame le nuove problematiche connesse all'adozione del regolamento generale europeo sulla protezione dei dati.

Come accennato, quando una relazione ha tali dimensioni non è possibile illustrarla, anche sinteticamente, ai lettori. Questa è la ragione per la quale ho scelto due particolari argomenti che credo possano essere di grande interesse ed attualità:

L'applicazione dei dettati del regolamento in ambito condominiale

L'autorità Garante in passato aveva più volte concentrato la sua attenzione su questo specifico contesto, che purtroppo spesso dà luogo ad acrimoniosi contenziosi fra i condomini.

Ancora una volta è stato confermato che il titolare del trattamento di qualunque tipo di dati, che riguardi le attività condominiale ed i condomini, è l'assemblea dei condomini nel suo complesso.

Questa assemblea può delegare, per la gestione quotidiana delle attività condominiali, con annesso trattamento di dati, un soggetto terzo, che nella grande maggioranza dei casi altro non è che l'amministratore del condominio. È già qui si presenta un problema, perché sono pochissime le assemblee condominiali che hanno compilato una lettera di designazione a responsabile del trattamento, indirizzata all'amministratore. Inoltre, in tale lettera di designazione dovrebbero essere indicate con chiarezza anche le modalità con cui è possibile migrare da un amministratore ad altro amministratore, con conseguente trasferimento di dati da un responsabile al successivo.

Sono temi che per solito non richiamano grande attenzione, finché non capita qualche grana, che spesso viene ripresa degli organi di comunicazione di massa e talvolta amplificata, anche in maniera non appropriata alle effettive circostanze sottostanti.

Il punto fondamentale a tenere presente, in fatto di trattamento di dati in contesto condominiale, è che l'assemblea è il titolare del trattamento e ciò significa che tutti i condomini sono contitolari del trattamento; a tali contitolari spetta l'obbligo di designare

per iscritto, previ specifici accertamenti, l'amministratore del condominio, che deve, nell'ambito delle sue attività, attenersi alle indicazioni dell'assemblea di condominio e del codice civile.

Inoltre, è facoltà dell'amministratore di condominio designare a sua volta degli autorizzati al trattamento, come ad esempio i soggetti che possono recarsi presso le singole unità immobiliari per acquisire dati afferenti a consumi idrici o energetici.

In questo contesto, se un condominio decide di installare un impianto di videosorveglianza, è evidente che l'assemblea è contitolare del trattamento e può delegare all'amministratore del condominio, in qualità di responsabile, la gestione dell'intero impianto, nonché all'eventuale recupero delle registrazioni, ove ciò sia richiesto dalle autorità di pubblica sicurezza o altri soggetti, che dovranno dimostrare le ragioni per le quali richiedono il recupero di questi dati. A questo proposito, ricordo che se un condomino chiede di recuperare i dati, ad esempio perché vittima di un furto, è opportuno che prima il condomino denunci l'accaduto alle forze di polizia e successivamente lasci che siano le forze di polizia ad occuparsi dell'acquisizione delle eventuali videoregistrazioni. Stessa cosa avviene se il furto avviene in danno di un inquilino e non di un proprietario.

La violazione dei dati

Il Garante ha tracciato una stringata panoramica dei contesti più frequenti.

Nel 2019 sono pervenute all'Autorità 1.443 notifiche di violazione dei dati personali, che hanno riguardato, come titolari del trattamento, soggetti pubblici (nel 27% dei casi) e soggetti privati (nel restante 73%). Le tipologie di violazione dei dati personali più frequenti, parte non irrilevante delle quali (avendo carattere transfrontaliero) sono state istruite mediante la piattaforma IMI (par. 21.1), hanno riguardato:

- *attacchi informatici volti all'acquisizione di dati personali (quali credenziali di accesso, dati relativi a strumenti di pagamento, dati di contatto);*
- *accesso non autorizzato a caselle di posta elettronica (ordinaria e certificata);*
- *perdita o indisponibilità di dati personali causata da malware di tipo ransomware;*
- *smarrimento o furto di dispositivi digitali o documenti cartacei contenenti dati personali;*
- *comunicazione o diffusione accidentale di dati personali.*

Ricordo ai lettori che il nuovo regolamento generale europeo prevede un notevole allargamento delle situazioni, nelle quali è indispensabile notificare l'accaduto all'autorità Garante. In precedenza, i casi in cui tale notifica era obbligatoria erano decisamente meno numerosi.

Durante le istruttorie, seguite alle notificazioni più significative, più volte si è messo in evidenza che la violazione di dati era conseguenza di insufficienti misure di sicurezza e questo fatto deve essere preso in adeguata considerazione da tutti i titolari e responsabili del trattamento, perché queste debolezze possono portare all'applicazione di sanzioni significative.

Un conto è un furto di dati, avveduto mediante scasso di una finestra e sottrazione di un PC portatile, un conto è un furto di dati, avvenuto quando il PC viene lasciato abbandonato sul sedile del passeggero di un'automobile. Vale la pena di ricordare a tutti, con l'occasione, che le conseguenze negative di entrambi questi furti potrebbero essere estremamente limitate, se solo si

provvedesse con maggior frequenza all'utilizzo di applicativi di criptografia, che sono oggi assai efficaci ed hanno un costo spesso nullo.

La relazione 2019 (pdf)

Adalberto Biasiotti

---

www.puntosicuro.it