Temi: Accesso ai dati
Categoria professionale: Direzione dei sistemi di sicurezza
Tipologia di dati: Privati

Posso utilizzare i dati dei miei clienti/utenti a scopo d'inchieste ?

Un organismo mette a disposizione dei suoi clienti/utenti un sito commerciale per ordinare articoli in linea. Per far ciò, sono loro richiesti un indirizzo e-mail e una password. Dopo qualche anno di esercizio, il sito recensisce circa un centinaio di clienti/utenti.
Il direttore dei sistemi d'informazione (DSI) dell'organismo decide di utilizzare questi dati a scopo d'inchieste. Interessato dalla sicurezza dei dati, desidera valersi del possesso di queste informazioni per investigare sulle precauzioni prese o meno dai suoi clienti/utenti: usano la stessa password per il loro conto di posta elettronica e per l'accesso alla vendita in linea?
Il DSI recupera le password dal sito di acquisto in linea e tenta di penetrare i conti di posta elettronica dei suoi clienti/utenti usando le password che hanno scelto per il sito commerciale. Prende certe misure volte a garantire il rispetto della vita privata dei clienti/utenti (non leggere i messaggi; non conservare la password, ecc.).
Messo al corrente di questa inchiesta, il suo superiore gli chiede di mettervi fine, sinché non abbia il consenso esplicito dei clienti/utenti. Sa che il metodo non è accettabile: le password sono confidenziali e non devono essere accessibili in nessun caso.
I dati raccolti per permettere l'acquisto in linea non possono essere usati per altri fini. Per di più, accedere indebitamente a un sistema informatico costituisce reato.

Raccomandazioni
I dati raccolti per un certo fine (permettere l'acquisto in linea) non possono essere usati per altri fini (investigare sul grado di sicurezza applicato dai clienti o dagli utenti). Questo principio vale per qualsiasi forma di ricerca o d'inchiesta, sia essa commerciale o scientifica. In questo caso, è necessario il consenso esplicito della persona interessata, perché non vi è un interesse preponderante privato o pubblico o delle leggi che permettano questo uso per altri fini. Le password non dovrebbero essere conservate non cifrate nella banca dati ma attraverso valori di "hachage" per essere messi in sicurezza e resi inaccessibili.

Prinicipi di base
LPD 4, 7, 12, 13, 14, 17; LIPAD 37 al.1 et 2; CP 143, 179novies

Liceità (legalità), sicurezza dei dati; trasparenza della raccolta, finalità.

Esempio concreto