Thèmes : Accès aux données
Métiers: Direction des systèmes d'information
Types de données: Privées

Puis-je utiliser les données de mes clients/usagers à des fins d'enquêtes ?

Un organisme met à disposition de ses clients/usagers un site commercial pour commander des articles en ligne. Pour ce faire, une adresse courriel et un mot de passe leur sont demandés. Après quelques années d'exploitation, le site recense quelques centaines de clients/usagers.
Le directeur des systèmes d'information (DSI) de l'organisme décide d'utiliser ces données à des fins d'enquêtes. Intéressé par la sécurité des données, il souhaite profiter de la possession de ces informations pour enquêter sur les précautions prises ou non par ses clients/usagers: utilisent-ils le même mot de passe pour leur compte de messagerie et pour l'accès à la boutique en ligne?
Le DSI récupère les mots de passe depuis le site d'achat en ligne et tente de pénétrer sur les comptes courriel de ses clients/usagers en utilisant les mots de passe qu'ils ont choisi pour le site commercial. Il prend certaines mesures pour garantir le respect de la vie privée des clients/usager (ne pas regarder les messages, ne pas conserver les mots de passe, etc.).
Mis au courant de cette enquête, son supérieur lui demande d'y mettre fin, tant qu'il n'a pas l'accord express des clients/usages. Il sait que la méthode n'est pas acceptable: les mots de passe sont confidentiels et ne doivent être accessibles en aucun cas.
Les données collectées pour permettre l'achat en ligne ne peuvent être utilisées à d'autres fins. De plus, accéder indûment à un système informatique constitue un délit.

Recommandations
Les données collectées à une certaine fin (permettre l'achat en ligne) ne peuvent pas être utilisées à d'autres fins (enquêter sur le degré de sécurité appliqué par les clients ou les usagers). Ce principe vaut pour toutes les formes de recherche ou d'enquête, qu'elles soient commerciale ou scientifique. En l'occurrence il faut le consentement explicite de la personne concernée, car il n'y a pas d' intérêt prépondérant privé ou public ou de lois permettant cette utilisation à d'autres fins. Les mots de passe ne devraient pas être conservés en clair dans la banque de données mais au travers de valeurs de "hachage" par exemple de manière à être sécurisés et inaccessibles.

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

Licéité (légalité), sécurité des données; transparence de la collecte, finalité

Ressources