Vol de données, perte de confiance

Me Sébastien Fanti, avocat et notaire, Expert IT Confédération Suisse

Depuis 2005, les rapports semestriels de la Centrale MELANI évoquent, de manière récurrente, le vol de données. Nonobstant cette tendance inquiétante, la réponse légale est souvent imparfaite, voire insolite.

Il convient, liminairement, de relever qu'avant que le vol de données ne survienne, souvent celui-ci a été précédé d'un hacking, soit d'un accès indu à un système informatique.
Le vol de données, respectivement l'infraction de soustraction de données fait l'objet d'un article spécifique du Code pénal, l'article 143 qui stipule: «Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.»
A la première lecture de la disposition légale, on perçoit la difficulté d'application liée, notamment, aux conditions émises par le législateur. Les données doivent faire l'objet d'une protection informatique, voire physique, visant à proscrire une soustraction de données diligentée de l'extérieur (firewall, antivirus, etc.), mais également de l'intérieur (de la part de collaborateurs ou de consultants notamment). Une interdiction contractuelle ou morale d'accéder aux données est donc totalement insuffisante dans ce dernier cas de figure.

En cas de doute sur l'existence d'un cas de vol de données, il convient de déposer une plainte contre inconnu.

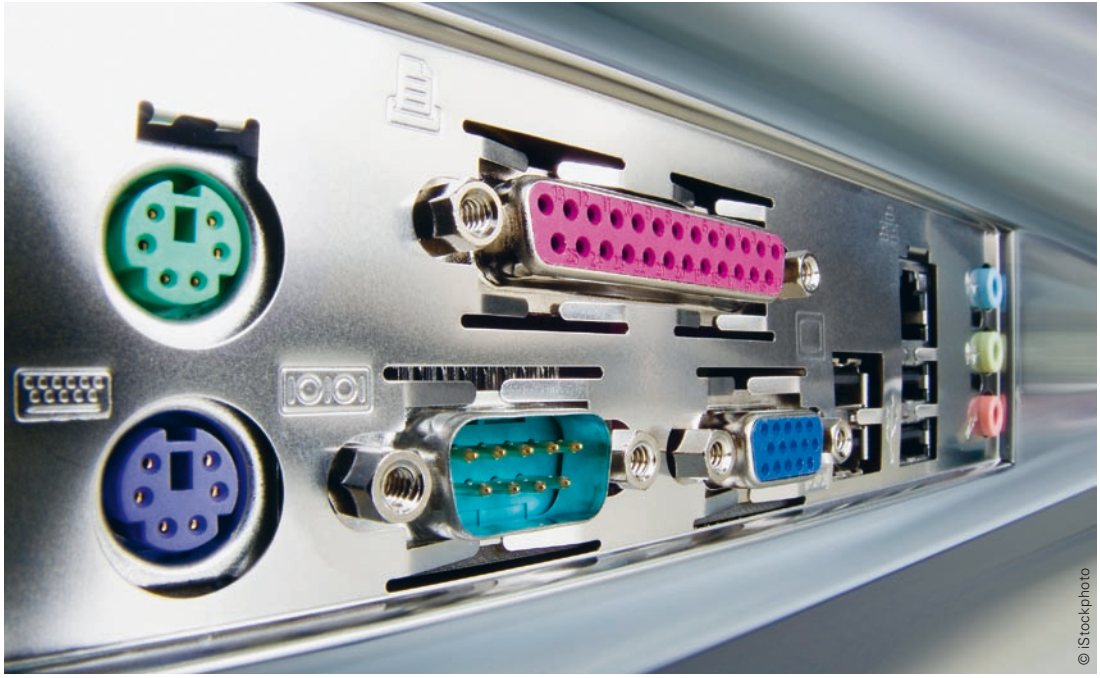
© iStockphoto

Une clause dans le contrat de travail ne suffit pas

Ainsi, une clause figurant dans un contrat de travail et proscrivant aux employés d'accéder aux données qui ne les concernent pas doit-elle être concrétisée dans les faits par une barrière informatique et/ou physique. A défaut, en cas de soustraction de données, l'issue sera défavorable sur le plan pénal, à tout le moins.
Demeure également ouverte la question de savoir si la personne qui procède par ingénierie sociale est punissable, ce qui ne semble pas être l'avis de la majorité de la doctrine. En sus, cette infraction n'est poursuivie que sur plainte, ce qui signifie que le délai pour soumettre de tels comportements à la justice pénale est très bref (3 mois). En cas de doute sur l'existence d'un cas de vol de données, il convient donc de déposer une plainte contre inconnu pour préserver l'ensemble de ses droits.

Moyens légaux dépassés

En définitive, les conditions actuelles d'application de cette disposition légale sont si restrictives que nombre de comportements échappent à une sanction pénale qui paraît à chacun justifiée. Ainsi, dans une affaire valaisanne, un employé qui avait soustrait les données relatives à des abonnés à un service de messagerie (login et mot de passe) a-t-il été acquitté de cette infraction, car aucune mesure de sécurité spécifique n'avait entravé son accès aux logiciels du back office, notamment. Cela n'est pas acceptable et le Tribunal l'a lui-même déploré en ces termes: «On peut s'interroger sur le sens de la protection restreinte accordée par le législateur dans sa volonté de renoncer à réprimer ce



Afin d'éviter de mauvaises surprises, il peut être envisageable d'interdire ou de limiter l'utilisation des supports de données amovibles.

qui équivaut à un abus de confiance au sens large du terme.» Les moyens légaux mis en œuvre, dès 1995, pour lutter contre la criminalité informatique sont donc non seulement dépassés au vu de l'évolution technologique, mais également au vu des comportements adoptés (vol d'identité numérique non punissable dans notre pays en vertu d'une disposition topique). Le Code pénal doit donc faire l'objet d'une révision urgente et les nouveaux types de délinquance informatique y être sanctionnés, par le biais de normes technologiquement neutres permettant une adaptation plus rapide dans un domaine où les révolutions numériques se succèdent à la fulgurance du net.

Conseils pour éviter le vol de données

L'une des conséquences mésestimées d'un vol de données est celle de la perte de confiance si, d'aventure, un tel vol devait être connu de tiers, voire de clients. La procédure pénale ne permet pas de réparer le dommage causé à l'image de l'entreprise. Mieux vaut donc faire appel à un professionnel pour la gestion de la communication de crise. Auparavant, il convient de prendre les mesures suivantes en application du principe de précaution:

- Adopter une charte sur l'utilisation des moyens informatiques et électroniques et l'adapter régulièrement en fonction de l'évolution des technologies implémentées (tablettes, cloud, etc.): même si cela ne suffit pas pour faire sanctionner un voleur de données sur le plan pénal, la voie civile nécessite un tel cadre juridique;
- Intégrer cette charte au contrat de travail qui doit, de surcroît, prévoir les sanctions en cas de violation;
- Sécuriser les données tant contre une intrusion externe que contre un vol survenant au sein même de l'entreprise: l'expérience enseigne que le danger que représente l'insider est connu, mais peu analysé en termes de sécurité informatique; des logiciels spécialisés (Data Loss Prevention) existent et leur coût est faible par rapport à celui d'un cas de vols avec toutes les conséquences envisageables (action civile des clients dont les données ont été volées, dénonciation au Préposé fédéral pour violation des normes garantissant la sécurité des données, procédure disciplinaire, etc.);
- Interdire ou limiter l'utilisation des supports de données amovibles (principalement les clés USB) qui ne laissent que peu de traces dans les systèmes d'exploitation; l'installation d'un logiciel de surveillance est une fois encore conseillée;
- Soumettre au Préposé fédéral à la protection des données pour validation tant les documents relatifs à la surveillance mise en place, que les procédures de surveillance et les outils utilisés: il faut éviter que l'employé indélicat puisse faire invalider les preuves recueillies au motif que la surveillance était illicite;
- En cas de doute sur l'existence d'un vol de données, ne rien modifier (préservation des preuves) et faire appel immédiatement à la police: les spécialistes se déplacent volontiers pour aider sur le terrain les entreprises à prendre les mesures qui s'imposent.

En définitive comme en toute chose, la voie médiane doit être privilégiée: utiliser les dernières technologies tout en se montrant respectueux de la vie privée et du droit de la personnalité. Cela passe par un usage accru de technologies susceptibles de collecter de manière automatisée les indices. L'intervention automatisée ne peut se voir reprocher d'être orientée.