

L a collecte déloyale de données à caractère personnel : petite mise au point ...

Les fondements légaux de cette infraction

L'essentiel

▸ Aux termes de l'article 6 de la loi Informatique et libertés modifiée en août 2004, « *les données sont collectées et traitées de manière **loyale et licite*** ».

▸ Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de **cinq ans d'emprisonnement** et de **300 000 euros** d'amende.

▸ Pour les **personnes morales**, la peine d'amende encourue est **quintuplée**, soit 1 500 000 euros, et s'accompagne des peines prévues à l'article 131-38 du Code pénal.

▸ Il n'existe **pas de définition légale** de la collecte déloyale. Le caractère déloyal de la collecte est donc laissé à l'appréciation du juge.

▸ La collecte d'informations auprès de tiers, **à l'insu des intéressés**, constitue une manœuvre déloyale, ces derniers n'ayant pas la possibilité de faire jouer leur droit d'opposition à la collecte (1).

La collecte de données personnelles, même si celle-ci a lieu sur des espaces publics de l'internet, implique de respecter strictement les obligations d'information des personnes telles qu'elles sont prévues par la loi Informatique et liberté. Faute de respecter ces obligations, la collecte pourra être qualifiée de déloyale et être constitutive d'une infraction pénale.

La collecte d'adresses e-mail sur les espaces publics de l'internet

▸ Dans une décision du **14 mars 2006** la Cour de cassation a considéré que la **collecte d'adresses électroniques** personnelles dans les espaces publics de l'internet constituait une collecte déloyale.

▸ La Cour estime **déloyal** le fait de collecter des adresses sans en avertir les titulaires, en ne les mettant pas en mesure de consentir à cette collecte et de faire valoir leurs droits à ce moment.

La tendance actuelle de la jurisprudence semble être la sévérité vis à vis des collecteurs de données négligents.

Les précautions à prendre dans la collecte des données

▸ Cette position de la Cour de cassation contraint toutes les **entreprises** susceptibles de telles collectes à mettre les **personnes concernées** en mesure de faire **valoir leurs droits** sur leurs données, lors de la collecte.

▸ La présence d'une donnée à caractère personnel sur un espace public ne signifie pas que cette dernière soit libre d'utilisation. Lors de la collecte, il convient de **s'assurer que les données peuvent être utilisées librement**.

(1) Cass. crim. 03/11/87.

Alain Bensoussan
alain-bensoussan@alain-bensoussan.com
Chloé Torres
chloe-torres@alain-bensoussan.com

Impact sectoriel

Autorisations uniques en matière de biométrie

L'enjeu

L'encadrement des dispositifs biométriques

▸ Aux termes de l'**article 25** de la loi Informatique et libertés modifiée, **la Cnil doit être sollicitée** pour donner son autorisation à la mise en place de solutions biométriques par des organismes, collectivités locales ou entreprises.

▸ Sont en effet mis en œuvre après autorisation « *les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes* ».

▸ Le **27 avril 2006**, la Cnil a adopté **trois autorisations uniques** en matière de biométrie.

▸ En ce qui concerne la méthodologie pratique, il suffira d'un **simple engagement de conformité**, qui peut être effectué en ligne, pour déclarer les traitements répondant aux normes d'autorisations uniques.

Ces normes d'utilisation unique répondent à une utilisation croissante des dispositifs biométriques. Ces autorisations permettent d'alléger considérablement les lourdeurs administratives liées aux procédures d'autorisation ; cependant, afin de garantir une protection adéquate des libertés individuelles, ces autorisations uniques ne concernent que des traitements biométriques sans dangers, puisque concernant uniquement des dispositifs sans traces.

Quels sont les traitements concernés ?

▸ La première autorisation concerne les traitements reposant sur la **reconnaissance du contour de la main** et ayant pour finalité le **contrôle d'accès** et la gestion des horaires et de la restauration sur le lieu de travail (1).

▸ La seconde autorisation concerne les traitements reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'**accès aux restaurants scolaires** (2).

▸ La troisième autorisation concerne les traitements reposant sur la **reconnaissance d'une empreinte digitale** exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'**accès aux locaux** sur les lieux de travail (3).

▸ Ces trois autorisations uniques définissent les **finalités**, les **caractéristiques** techniques, les **données traitées**, la **durée** de conservation des données, les **moyens de sécurité** et les **droits des personnes** concernées caractérisant la mise en œuvre de ce type de traitements.

▸ Les responsables des traitements peuvent procéder à la déclaration de conformité à l'aide d'un formulaire **accessible sur le site www.cnil.fr**.

(1) Norme n°AU007, délib.n° 2006-101 du 27/04/2006.

(2) Norme n°AU009, délib.n° 2006-103 du 27/04/2006.

(3) Norme n°AU008, délib.n° 2006-102 du 27/04/2006.

Les FAQ juristendances

Sources

Est-il nécessaire de déclarer les fichiers constitués à des fins d'information ou de communication externe ?

▸ **Non**, la Cnil a adopté le 9 mai 2006, une délibération dispensant de déclarations les fichiers constitués à des fins d'information et de communication externe.

▸ Auparavant ces fichiers pouvaient bénéficier d'une déclaration simplifiée, s'ils entraient dans le cadre de la norme simplifiée n° 15.

▸ Dorénavant les **listes d'adresses**, de contacts et de correspondants constituées par des organismes publics ou privés **à des fins d'information** ou de communication externe pourront être **dispensées de déclaration** si ces traitements respectent les conditions fixées par la Cnil dans sa délibération (1).

(1) Délibération n°2006-138 du 9 mai 2006
(dispense de n°7)

▸ La Cnil rappelle que cette dispense de déclaration ne s'applique pas aux fichiers ayant pour objet l'envoi de sollicitations commerciales ou le démarchage politique ou électoral.

www.cnil.fr

Les fichiers de membres et de donateurs d'association doivent-ils être déclarés à la Cnil ?

▸ **Non**, la Cnil a pris le 9 mai 2006, la décision de dispenser de déclaration préalable les fichiers de membres et de donateurs d'association.

▸ Auparavant, ces fichiers devaient être déclarés sous forme simplifiée en respectant les exigences de la norme simplifiée n° 23.

▸ La diffusion sur internet de l'**annuaire des membres d'une association**, les sites web d'association ou encore l'utilisation à des fins de prospection des fichiers de membres et de donateurs d'associations peuvent désormais être faits **sans déclaration préalable** auprès de la Cnil (2).

(2) Délibération n°2006-130 du 9 mai 2006
(dispense n°8)

▸ Certains fichiers d'association restent toutefois soumis à une formalité préalable, comme ceux comportant des données sensibles ou ceux utilisés à des fins de prospection politique.

www.cnil.fr

Actualité

La Cnil autorise les expérimentations du dossier médical personnel

Sources

▸ Le **30 mai 2006**, la Cnil a autorisé les applications informatiques mises en œuvre au sein des **établissements de soins** et par les **professionnels de santé** participant à l'expérimentation du dossier médical personnel (DMP) (1).

▸ La finalité principale de l'expérimentation du DMP sera de **tester la faisabilité et l'acceptabilité** du dispositif envisagé.

▸ La Cnil a autorisé l'expérimentation, en rappelant sa préoccupation sur l'importance des **mesures de sécurité** mises en œuvre par les **hébergeurs du DMP**, et en insistant sur le fait que la sécurité est une recommandation constante en matière de **bases de données sensibles**.

(1) Cnil, Echos des séances du 30 mai 2006, www.cnil.fr

Condamnation d'une société qui, à travers un sondage prétendument anonyme, avait collecté des données personnelles sensibles

▸ En juin 2004, le **Tribunal correctionnel de Nanterre** a condamné le dirigeant d'une société qui avait adressé un courrier électronique présenté sous la forme d'un **sondage politique anonyme** pour, en fait, recueillir des adresses électroniques et d'autres données personnelles (2).

(2) Cnil, Echos des séances du 30 mai 2006, www.cnil.fr

▸ La société a été reconnue coupable de l'infraction de **collecte** de données nominatives **par un moyen frauduleux**, déloyal ou illicite, d'enregistrement et conservation de données nominatives sensibles sans l'accord des intéressés et de **détournement de la finalité** d'un traitement automatisé d'information nominative. Elle s'est **désistée de son appel** en avril (3).

(3) CA Versailles, 26 avril 2006.

Adoption du nouveau règlement intérieur de la CNIL

▸ La Cnil a adopté le **23 mai 2006** un nouveau règlement intérieur dans lequel sont apportées des précisions sur le décret du 20 octobre 2005 (4).

(4) Délibération n°2006-147 du 23 mai 2006 www.cnil.fr

▸ Il précise entre autre, la **communicabilité** des décisions de la Cnil et les règles d'**incompatibilité** pour les agents amenés à faire des contrôles.

Directeur de la publication : Bensoussan Alain
Rédigée et animée par Chloé Torres et Isabelle Pottier
Diffusée uniquement par voie électronique
ISSN (en cours)
Abonnement à : avocats@alain-bensoussan.com