

DONNÉES CLIENTS

DES TRAITEMENTS SOUMIS À AUTORISATION DE LA CNIL



Héléne Lebon

Avocat
Bird & Bird

La nouvelle loi Informatique et Libertés soumet certains traitements comportant des données à caractère personnel à une autorisation de la CNIL. Cette dernière a adopté une interprétation large de ces dispositions, qui concernent un nombre toujours plus important de traitements.

Depuis le vote de la réforme de la loi Informatique et Libertés au mois d'août 2004, certains traitements comportant des données à caractère personnel ne peuvent être mis en œuvre qu'après que son responsable a obtenu l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL). L'analyse des délibérations adoptées par la Commission démontre qu'un grand nombre de traitements mis en

œuvre par les organismes bancaires et financiers sont soumis à cette autorisation préalable de la Commission qui considère que doivent faire l'objet d'une telle formalité les traitements susceptibles d'exclure les personnes du bénéfice d'un contrat.

DÉCLARATIONS SIMPLIFIÉES...

Pour les traitements soumis à déclaration, l'article 24 de la loi prévoit que la CNIL peut cependant adopter des normes simplifiées, permettant aux organismes qui disposent de traitements entrant strictement dans le cadre de ces normes de procéder à des formalités simplifiées. Toutefois, l'article 24 précité précise que seuls les traitements ne portant pas atteinte aux libertés des personnes peuvent faire l'objet d'une norme simplifiée. La CNIL a adopté au cours des dernières années des normes relatives à la mise en œuvre des comptes clients, à la gestion des crédits, ou encore à la gestion des instruments financiers. Cependant, force est de constater que ces normes ne correspondent plus aux traitements très sophistiqués mis

en œuvre par les organismes bancaires et financiers de nos jours... Alors même que ceux-ci estiment très souvent que les traitements de données personnelles portant sur leurs clients qu'ils mettent en œuvre entrent dans ce cadre de normes simplifiées. Or la réforme de la loi a inséré dans le Code pénal un article 226-16-1-A qui sanctionne d'une peine de 5 ans d'emprisonnement et de 300 000 euros d'amende le fait, pour un responsable de traitement, d'avoir déclaré sous la forme d'une déclaration simplifiée un traitement qui n'était pas conforme à la norme simplifiée de référence.

OU AUTORISATIONS UNIQUES...

Pour les traitements soumis à autorisation préalable de la CNIL, la Commission dispose du pouvoir d'adopter des documents appelés "autorisations uniques" qui permettent aux responsables mettant en œuvre des traitements soumis à autorisation, de procéder à des formalités simplifiées, à la condition – là aussi – que les traitements envisagés entrent strictement dans le cadre des autorisations uniques adoptées par la CNIL. L'adoption de ces autorisations uniques a été l'occasion pour la CNIL de faire connaître sa position sur les traitements soumis à autorisation. Les traitements devant faire l'objet d'une autorisation de la CNIL dans le monde bancaire sont notamment "les traitements automatisés susceptibles, du fait de leur nature, de leur portée, ou de leurs finalités, d'exclure des personnes du béné-

REPÈRES

Le dispositif de la CNIL

■ Les traitements soumis à déclaration

- la déclaration ordinaire : cas général
- la déclaration simplifiée concerne les traitements de données correspondant à une norme simplifiée établie par la CNIL. Ces normes portent sur "les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés".

■ Les traitements soumis à autorisation

- l'autorisation de traitement unique : les traitements soumis à demande d'autorisation sont listés par l'article 25 de la loi ;
- l'autorisation unique de traitements correspond à des traitements qui ont une même finalité, portent sur des catégories de données identiques et s'adressent aux mêmes destinataires.

fice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire" (article 25 I 4°); mais aussi les traitements automatisés ou non (c'est-à-dire les traitements informatisés ou sur papier) "portant sur des données relatives aux infractions, aux condamnations, ou aux mesures de sûreté" (article 25 I 3°); ou encore les interconnexions de traitements dont les finalités principales sont différentes (article 25 I 5°).

UN CHAMP LARGE D'APPLICATION

Ainsi, par une délibération en date du 2 février 2006, la CNIL a adopté une autorisation unique portant sur la mise en place de traitements permettant d'aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit. La Commission considère en effet que de tels traitements sont soumis à son autorisation préalable sur le fondement de l'article 25 I 4° de la loi Informatique et Libertés dans la mesure où – selon la CNIL – ces scores sont "susceptibles d'exclure, au moins de façon temporaire, une personne du bénéfice d'un contrat de crédit".

De même, par une délibération en date du 1^{er} décembre 2005, la CNIL a adopté une autorisation unique dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme, pour des traitements dont la mise en œuvre est pourtant imposée par le respect des dispositions du Code monétaire et financier. La CNIL estime en effet que, même si la lutte contre le blanchiment des capitaux et le financement du terrorisme est une obligation légale, la constatation de l'existence de blanchiment de capitaux conduit le plus souvent les établissements à rompre leurs relations contractuelles avec les personnes concernées. Il convient également de constater que le blanchiment de capitaux constitue une infraction réprimée par l'article L. 324-1 du Code pénal, dès lors que

les traitements (y compris sur papier) comportant des données sur des infractions sont soumis à autorisation préalable de la CNIL sur le fondement de l'article 25 I 3° de la loi Informatique et Libertés.

LE CAS DES TRAITEMENTS AUTOMATISÉS

Au-delà des autorisations uniques qu'elle adopte, la CNIL affirme sa position à l'occasion de formalités effectuées par les établissements. Ainsi, par une délibération en date du 21 décembre 2006, la CNIL a considéré qu'un traitement automatisé permettant à un établissement d'enregistrer le numéro de carte bancaire des clients qui payent par ce moyen, à des fins de prévention des risques de fraudes, est soumis à son autorisation préalable dans la mesure où le système pourra conduire au blocage de la carte ce qui empêchera le client de l'utiliser. Dans un autre secteur d'activité, la CNIL a considéré qu'un traitement automatisé mis en place par une caisse d'assurance maladie ayant pour finalité la gestion des contentieux et des litiges est également soumis à son autorisation préalable (délibération n° 2007-037). La CNIL pourrait raisonner par analogie et considérer que de tels traitements mis en œuvre par un organisme financier sont soumis à son autorisation.

LES TRANSFERTS DE DONNÉES

Comme tous les autres responsables de traitements, les organismes bancaires et financiers procédant à des transferts de données personnelles vers un pays tiers à l'Union européenne ne disposant pas d'un niveau de protection suffisant sont généralement soumis à l'autorisation préalable de la CNIL. Ainsi la Commission a déjà autorisé des organismes financiers à transférer des données personnelles hors de l'Union européenne dans le cadre du recours à un prestataire situé

au Maroc (délibération n° 2007-176), dans le cadre d'organisation d'opérations de prospection commerciale (délibération n° 2007-059).

Bien entendu, la CNIL peut refuser en partie ou en totalité de tels transferts : ainsi par une délibération en date du 8 février 2007, elle a refusé à une filiale française d'une société américaine l'autorisation de transférer aux États-Unis la copie scannée des pièces d'identité des clients français.

SUR LES DISPOSITIONS DU RÈGLEMENT GÉNÉRAL DE L'AMF

Les traitements mis en œuvre pour permettre aux organismes bancaires et financiers d'appliquer les textes entrés en vigueur récemment pourraient également être considérés comme devant faire l'objet de l'autorisation préalable de la CNIL. En effet, l'interprétation large de l'article 25 de la loi Informatique et Libertés pourrait la conduire à considérer que les traitements permettant d'évaluer les connaissances des clients des prestataires de services d'investissement, en application des dispositions des articles 314-44 et suivants du règlement général de l'AMF, doivent faire l'objet de son autorisation préalable dans la mesure où ces traitements conduiront ces prestataires à ne pas proposer aux clients néophytes certains placements risqués. De la même manière, la CNIL pourrait considérer que la mise en place de traitements (y compris les traitements tenus sur fichiers papier) permettant de détecter ou de recenser les abus de marché sont également soumis à son autorisation préalable dans la mesure où ces systèmes comporteront nécessairement des données sur des infractions. Cette position de la CNIL semble par conséquent soumettre à son autorisation préalable un nombre toujours plus important de traitements mis en œuvre par les organismes bancaires et financiers dans le cadre de la gestion des données sur les clients. ■

“La CNIL a adopté une autorisation unique sur la mise en place de traitements permettant d'aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit.”