La loi Informatique et Libertés, modifiée en août 2004, donne à la CNIL le pouvoir de soumettre au régime d'autorisation préalable les traitements de données liés à la lutte contre le blanchiment et le financement du terrorisme. L'adoption du principe de la décision unique permet d'alléger ces formalités. Cependant cette nouvelle procédure ne s'applique a priori qu'aux traitements expressément décrits dans la loi, dans un domaine où la réglementation et les pratiques sont fortement évolutives. Comment éviter cette rigidité ? Olivier Coutor (CNIL) explique que ces nouvelles modalités d'intervention de la CNIL ne sont qu'une première étape dans une démarche qui sera nécessairement progressive. Pour Raoul d'Estaintot (Confédération Nationale du Crédit Mutuel), la délibération de la CNIL est difficilement applicable en l'état, car en contradiction avec les obligations des banques en matière de lutte contre le blanchiment. Laurent Caron (avocat), en revanche, montre comment interpréter le cadre actuel pour lui donner la souplesse nécessaire tout en préservant la sécurité juridique.

LUTTE ANTI-BLANCHIMENT ET PROTECTION DES DONNÉES
Les dernières réponses de la CNIL

Olivier Coutor

Chargé de mission direction juridique **CNIL**

L'utilisation de données dans le cadre de la lutte anti-blanchiment est soumise à l'autorisation de la CNIL. Pour alléger les formalités, celles-ci instaure une procédure d'autorisation unique fixant un cadre règlementaire qui, s'il est respecté, permet d'obtenir une autorisation de mise en œuvre sans contrôle a priori.

La délibération du 1er décembre 2005 de la CNIL est révélatrice de l'une de ses nouvelles formes d'interventions* : l'application de la procédure d'autorisation préalable par la Commission à certains types de traitements du secteur privé, définis en fonction des catégories de données qui y sont traitées (par exemple, les données relatives à des infractions, les données biométriques, le numéro de sécurité sociale), de la nature des finalités poursuivies ou des conséquences envisageables pour les personnes concernées (exclusion du bénéfice d'une prestation) ou encore de l'existence d'interconnexions entre des traitements ayant des finalités principales différentes.

Pour exercer au mieux cette nouvelle mission, mais aussi pour éviter un allongement excessif des délais d'instruction opposés aux organismes déclarants, la CNIL a décidé de recourir dans la mesure du possible à la procédure d'autorisation unique prévue au II de l'article 25. Les textes qu'elle peut adopter à ce titre ne sont rien d'autre que des cadres réglementaires auxquels tout responsable d'un traitement peut se référer sous réserve de s'engager sur la conformité de son traitement aux conditions et obligations définies par la CNIL. Cette procédure ne peut donc pas être suivie lorsque le traitement ne répond pas à certaines des conditions posées par l'autorisation unique ou s'il inclut des spécificités qui n'y sont pas prévues. Cependant, si rien n'interdit aux déclarants de préférer présenter un dossier particulier de demande d'autorisation, il n'en reste pas moins que les autorisations uniques ont vocation à servir de cadre de référence.

Pour ces raisons, la CNIL a souhaité faire précéder l'adoption de ces textes d'une phase approfondie de concertation avec les professionnels concernés. Pour ce qui concerne l'autorisation unique consacrée aux traitements de lutte anti-blanchiment, la Commission bancaire, la cellule de renseignement financier Tracfin, la Fédération bancaire française (FBF) et l'Association française des sociétés financières (ASF) ont été consultées et un bon nombre de leurs observations prises en compte.

LES RÈGLES DE FOND

La délibération de la CNIL est bâtie sur quelques-uns des principes de la loi du 6 janvier 1978, qui trouvent ainsi leur traduction dans le domaine de la lutte anti-blanchiment :

- **la définition des finalités d'un traitement par référence aux dispositions légales qui les régissent,** ce qui, en l'espèce, a conduit à ne retenir, à l'article 1er de la délibération, que les critères posés par la loi pour caractériser les requêtes informatiques qui permettront de détecter, au sein des traitements de tenue des comptes de la clientèle, les opérations financières devant faire l'objet d'une surveillance spécifique ;
- **la détermination des catégories de données à caractère personnel susceptibles d'être traitées** et de leur durée de conservation en fonction non seulement de leur utilité au regard de la finalité énoncée (par applica-

* Issues de la loi du 6 août 2004 qui a modifié la loi du 6 janvier 1978 dite "Informatique et Libertés".

tion du principe d'adéquation et de pertinence des données traitées) mais aussi d'un critère de proportionnalité (l'article 6 de la loi de janvier 1978 ajoute que les données traitées ne doivent pas être excessives au regard des finalités poursuivies) ;

- **la préservation de la confidentialité des données,** ce principe étant en l'espèce renforcé au plan légal puisqu'il est pour partie opposable au client concerné par un signalement anti-blanchiment ; ceci a notamment conduit à rappeler à l'article 3 que l'existence d'une déclaration de soupçon adressée à Tracfin et les suites qui lui sont réservées ne sont pas communicables aux autres services anti-blanchiment au sein d'un même groupe bancaire, ni a fortiori en dehors du territoire national, ce qui ne s'oppose pas à la circulation des données brutes qui sont portées dans ces déclarations comme des autres éléments factuels connus des services anti-blanchiment ; le débat actuel sur l'interprétation des textes en vigueur (cf. article de M. d'Estaintot) ne trouvera sa solution que le jour où un accord aura été trouvé sur leur portée avec les différentes autorités publiques intervenant en matière de lutte anti-blanchiment, la CNIL ne pouvant intervenir ici que pour faciliter l'adoption de cette solution ; au-delà de ce débat particulier, il n'y a pas lieu de s'étonner que les délibérations de la CNIL, lorsqu'elles portent sur des traitements effectués pour l'application de dispositions légales, servent parfois à révéler des désaccords dans leur interprétation entre les personnes concernées ; il va cependant de l'intérêt de toutes les parties que ces problèmes soient résolus dans les meilleurs délais.
- **l'élimination de tout obstacle à la libre circulation des données** lorsque celles-ci sont transférées vers un État qui assure un niveau de protection des données jugé suffisant, seule hypothèse incluse dans le champ de l'autorisation unique ;
- **l'information systématique des personnes sur les modalités de traitement des données qui les concernent :** les clients doivent être avertis, notamment au moment de l'entrée en relation, des finalités précises des traitements que la banque met en œuvre, en l'espèce pour répondre à ses obligations légales ;
- **la mise en place de procédures qui permettront aux personnes physiques** d'exercer leurs droits de vérifier la nature et la qualité des données traitées les concernant et de les faire rectifier, si nécessaire.

LE DROIT D'ACCÈS

Cette question semble être actuellement la plus difficile à régler. Par principe, les droits d'accès et rectifications peuvent être directement exercés par leurs titulaires sans qu'ils aient l'obligation de demander l'intervention d'un tiers (droit d'accès direct). Or, en l'espèce, l'exercice de ce droit d'accès pourrait, dans certains cas, remettre en cause l'efficacité de la lutte contre le blanchiment en permettant à ceux qui se prêtent à de telles opérations d'organiser leur riposte.

C'est un raisonnement de même nature qui a conduit à prévoir, au sein de la loi Informatique et Libertés, un régime de droit d'accès indirect : la personne concernée peut seulement, vis-à-vis de certains traitements, demander à un magistrat de la CNIL de contrôler à sa place les informations la concernant qui y sont enregistrées. Ce dispositif s'applique en particulier aux traitements intéressant la sécurité publique, la sûreté de l'État ou la Défense. Le magistrat de la CNIL peut vérifier la pertinence des données traitées et le respect des durées de conservation prévues, les faire effacer ou rectifier si nécessaire et éventuellement demander que tout ou partie des informations, jugées moins sensibles, soient communiquées au requérant.

« La CNIL envisage d'étendre peu à peu le texte à de nouveaux traitements ou fonctionnalités, au fur et à mesure que la Commission estimera pouvoir garantir leur conformité avec la loi Informatique et Libertés. »

Cependant, le régime du droit d'accès indirect des articles 41 et 42 de la loi du 6 janvier 1978 ne peut pas, en l'état actuel des textes, s'appliquer aux traitements des organismes financiers quant bien même leur finalité serait liée à l'exercice d'une mission de contrôle, d'intérêt général. Par ailleurs, si le Code monétaire et financier comporte bien des dispositions (articles L. 563-3 et L. 574-1) qui interdisent d'informer le client sur la surveillance dont il est l'objet, leur champ d'application n'est pas aisé à délimiter au sein des traitements couverts par l'autorisation unique. Ceci a conduit la CNIL à proposer aux organismes qui seraient saisis par un client ou un ancien client d'une demande de droit d'accès portant sur les données le concernant qui figurent dans les traitements de lutte anti-blanchiment, de l'interroger pour connaître son avis sur la nature des renseignements à communiquer au requérant et, éventuellement, de s'y référer dans leur réponse.

Il ne s'agit cependant que d'une solution de court terme qui ne peut prétendre pallier l'inadaptation des règles de droit d'accès en vigueur à l'égard des données traitées au titre de l'obligation de vigilance en matière de lutte contre le blanchiment. L'insécurité juridique qui pèse actuellement sur les établissements financiers ne disparaîtra pleinement que lorsque le Code monétaire et financier comportera une disposition instaurant, pour certaines des informations incluses dans ces traitements, à définir avec précision, un mécanisme proche du droit d'accès indirect de l'article 41 de la loi du 6 janvier 1978. Il serait utile que les représentants des professionnels concernés s'attachent à sensibiliser les pouvoirs publics sur cette difficulté qui ne doit pas être sous-évaluée. Des initiatives convergentes pourraient être prises pour chercher

au plan légal une solution équilibrée, qui exclurait de soumettre au régime de droit d'accès indirect la totalité des données figurant dans les traitements de lutte anti-blanchiment.

L'AVENIR PROCHE

Cette autorisation unique n'a pas vocation à rester figée une fois pour toutes. Elle est au contraire appelée à évoluer dans le cadre d'une démarche progressive. En réalité, nous n'en sommes qu'à la première étape d'un processus qui vise à éviter deux écueils : figer la position de la CNIL, ce qui serait d'autant plus une erreur que de nouveaux textes apparaissent régulièrement en matière de lutte anti-blanchiment ; refuser d'élargir le champ de l'autorisation unique alors même que celle-ci ne saurait prétendre aujourd'hui couvrir la totalité des traitements des organismes financiers liés à la lutte contre le blanchiment. Bien au contraire, la CNIL envisage d'en étendre peu à peu le champ à de nouveaux traitements ou fonctionnalités, au fur et à mesure que la Commission estimera en avoir une bonne connaissance et pouvoir garantir leur conformité avec la loi Informatique et Libertés.

La réflexion de la CNIL se concentrera dorénavant sur les dispositifs de filtrage qui ne correspondent pas à des critères fixés par la loi, sur le recours à des systèmes de score en matière de lutte anti-blanchiment, sur les "listes noires" externes, souvent d'origine anglo-saxonne, de personnes présumées à risque, auxquelles nombre d'organismes souhaitent recourir pour les aider dans l'accomplissement de leurs obligations de vigilance, sur le contenu des fichiers de "personnes politiquement exposées", ainsi que sur les traitements des organismes non bancaires également soumis aux obligations de la lutte anti-blanchiment. Autant de traitements qui, dans l'immédiat, continueront à devoir faire l'objet d'une autorisation au cas par cas. ■

Raoul d'Estaintot

Responsable de la cellule Prévention des fraudes
Confédération Nationale du Crédit Mutuel *

La contradiction issue de la délibération CNIL

Une délibération de la CNIL interdit la mutualisation des déclarations de soupçon au sein des groupes bancaires, ce qui n'est pas compatible avec les obligations des banques dans le cadre de la lutte contre le blanchiment. La profession bancaire souhaite que ce texte soit modifié pour permettre ce partage d'informations.

La position de la CNIL, exposée dans sa délibération du 1er décembre 2005 [1], conduit à s'interroger sur la portée du secret bancaire et, ensuite, sur les conséquences de cette position.

Celle-ci édicte que les services de lutte contre le blanchiment des entités composant un groupe ou un conglomérat ne peuvent pas avoir accès aux éléments relatifs aux déclarations de soupçon transmises à Tracfin ni aux suites qui leur sont réservées.

La délibération de la CNIL renvoie explicitement à l'article L. 511-34 du Code monétaire et financier qui stipule que les organismes financiers établis en France et faisant partie d'un groupe ou d'un conglomérat sont obligés de transmettre aux banques et entreprises d'investissement de leur groupe, sis en France, dans l'Union européenne ou dans l'EEE, "*les informations nécessaires à l'organisation de la lutte contre le blanchiment des capitaux et contre le financement du terrorisme*". L'article R.562-2-1 du même Code [2], précise que cet échange d'informations comprend également les données relatives à la clientèle.

L'article L. 511-34 est compris dans la section du Code consacrée au secret professionnel. L'article précédent (L. 511-33) pose le principe d'un secret absolu mais qui est levé à l'égard de la Commission bancaire, de la Banque de France et de l'autorité judiciaire agissant dans le cadre d'une procédure pénale. Des dispositifs législatifs peuvent, spécialement, déroger à ce principe. Ainsi, le Code monétaire

*** C'est à ce dernier titre que Raoul d'Estaintot présente une des particularités de la délibération de la CNIL concernant les traitements de données liés à la lutte contre le blanchiment des capitaux et contre le financement du terrorisme.**

et financier prévoit la levée du secret bancaire à l'égard de Tracfin pour lui adresser des déclarations de soupçon à condition qu'elles soient faites de bonne foi. En revanche, il édicte l'interdiction pour la banque déclarante d'informer le client de la déclaration de soupçon portant sur une ou plusieurs de ses opérations sous peine d'engager sa responsabilité pénale. De même, Tracfin et les autorités de contrôle sont astreints au secret professionnel et ne peuvent communiquer ces informations que dans une optique de lutte contre le blanchiment et de financement du terrorisme.

LA LEVÉE DU SECRET BANCAIRE EN QUESTION

Se trouve donc posée la question de la levée du secret bancaire édictée par l'article L. 511-34. En effet, cet article, venant après l'article L. 511-33, peut être compris comme une dérogation au principe de secret qui vient d'être énoncé. Ce qui est secret ne peut couvrir ni une organisation ni des procédures de lutte anti-blanchiment et de lutte anti-terroriste comme pourrait le laisser penser la formulation de l'article L. 511-34. De fait, l'organisation dans ces domaines n'est nullement confidentielle puisque la réglementation oblige la nomination de correspondants Tracfin qui doivent être connus de l'ensemble du personnel, des autorités de tutelle et de Tracfin, la mise en place d'une direction de la conformité, de contrôles périodique et permanent, d'un service de lutte anti-blanchiment... De même, les procédures de lutte anti-blanchiment et de lutte anti-terroriste ne sont que la déclinaison des obligations réglementaires édictées par le titre VI du livre V du Code monétaire et financier. Dans la mesure où le décret du 26 juin 2006 signale que l'information doit concerner les données nominatives de la clientèle, cette précision enlève toute ambiguïté et doit être interprétée comme incluant les informations figurant dans les déclarations de soupçon. Au demeurant, on se demande comment le corps d'inspection d'un organe central ou d'un siège pourrait contrôler la pertinence d'un dispositif de lutte anti-blanchiment, sa conformité avec le Code monétaire et financier et le niveau de risque de blanchiment sans pouvoir analyser le contenu des déclarations de soupçon émises par les différentes composantes du groupe.

LES CONSÉQUENCES DE LA POSITION DE LA CNIL

Le Code monétaire et financier précise, dans son article L. 562-2, qu'une déclaration de soupçon est faite sur une somme ou sur une opération portant sur une somme. Les éléments internes à une déclaration de soupçon concernent donc, notamment, le nom de l'établissement émetteur, le nom du client et les informations s'y rapportant ainsi que le mode opératoire. La délibération de la CNIL revient à autoriser la centralisation des déclarations de soupçon, mais sans avoir accès à leurs éléments matériels. Autrement dit, il s'agit d'un simple stockage qui ne permet ni au groupe de connaître ses propres typologies de blanchiment dont il peut être victime, ni de dresser un profil de risque de blanchiment de sa clientèle, ni même d'avoir un outil de pilotage de la prévention du risque de blanchiment à partir de l'analyse des déclarations (par émetteur, niveau de montant, mode opératoire...).

En conséquence, ne pouvant connaître les circuits de blanchiments utilisés à son insu, le groupe ne sera pas en mesure d'ajuster ses procédures, de mettre en place des détecteurs ou d'en affiner les paramètres. De même, il ne pourra pas dresser un profil de risque de blanchiment d'un client qui serait en relations d'affaires avec plusieurs entités du groupe. De fait, ce client est à même d'avoir plusieurs statuts : être un risque avéré dans la ou les entités ayant fait une déclaration de soupçon ; être un risque "naissant" dans les autres entités ayant détecté un mouvement remarquable, mais dont les recherches ne conduisent pas, à ce stade de l'investigation, à faire une déclaration à Tracfin ou ne représentent aucun risque de blanchiment du fait de l'absence de mouvement suspect.

« En conséquence, ne pouvant connaître les circuits de blanchiments utilisés à son insu, le groupe ne sera pas en mesure d'ajuster ses procédures. »

SUPPRIMER TOUTE AMBIGUÏTÉ

Il convient de savoir si la position de la CNIL serait soutenue par un juge d'instruction. En effet, il n'est pas exclu que, constatant, dans un groupe, la non-mise en œuvre du partage d'informations, il en tire les conséquences selon lesquelles ce manquement relève d'une volonté délibérée du groupe et engage la responsabilité pénale de la ou des personnes morales concernées, de leurs dirigeants et préposés. Inversement, la mise en œuvre de ce partage d'informations, alors que la délibération de la CNIL l'interdit, pourrait valoir aux mêmes personnes morales et physiques leur mise en cause pénale. Enfin, le non-respect de cette obligation légale de partage d'informations pourrait conduire la Commission bancaire à qualifier ce manquement de "*grave défaut de vigilance*" ou de "*carence dans l'organisation*" des procédures internes de contrôle du groupe et la conduire à ouvrir une procédure disciplinaire. Elle doit alors en aviser le procureur de la République (article L. 562-7). Afin d'éviter toute ambiguïté d'interprétation de la délibération de la CNIL, il convient de modifier l'alinéa litigieux de l'article 3 pour permettre aux services de lutte anti-blanchiment des entreprises composant le groupe de prendre connaissance des déclarations de soupçon émises par chacune d'entre elles. Il suffit de supprimer le

[1] Portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre au titre de la lutte contre le blanchiment et le financement du terrorisme.
[2] Créé par le décret n° 2006-736 du 26 juin 2006.

renvoi au *e)* à l'alinéa 3 de l'article 3 qui serait ainsi rédigé : "*les destinataires visés au f) ne peuvent avoir accès aux éléments relatifs aux déclarations de soupçon…*" Cela aurait aussi l'avantage de permettre au groupe de pouvoir mettre en place un véritable dispositif d'intelligence économique reposant sur le partage d'informations. Certes, il conviendra de bien encadrer une telle démarche en prévoyant des droits d'accès, des habilitations – celles-ci existent déjà puisque les correspondants Tracfin doivent être désignés par les dirigeants et leur nom est communiqué à la Commission bancaire et à Tracfin –, des contrôles, voire une charte déontologique destinée aux équipes des services de lutte anti-blanchiment pour faire en sorte que la finalité de la lutte contre le blanchiment et le financement du terrorisme soit respectée.

ORGANISER LE PARTAGE D'INFORMATIONS

Il ne s'agit pas de sacrifier à un effet de mode, mais tout simplement d'offrir aux services de lutte anti-blanchiment des composantes d'un groupe une aide à la décision et de leur permettre d'être plus réactifs. Ce partage d'informations contribue également à la consolidation de la surveillance du risque de blanchiment et de la connaissance de la clientèle ainsi que le préconisent le Comité de Bâle et la Commission bancaire. Enfin, cette démarche se situe dans les évolutions de la 3e directive (article 28) qui prévoit le partage d'informations y compris entre banques ne faisant pas partie d'un même groupe. Ainsi, ce ne peut être que dans le sens du partage d'informations à l'intérieur d'un groupe, en y intégrant les déclarations de soupçon, que doit être compris l'article L. 511-34 créé par la loi de sécurité financière du 1er août 2003. ■

Comment utiliser l'autorisation unique de la CNIL ?

Laurent Caron

Avocat à la Cour
Associé
Lamy & Associés

Les nouvelles modalités d'intervention de la CNIL dans le cadre de la lutte anti-blanchiment peuvent s'interpréter comme un socle de conformité a minima. Ce qui laisserait ouverte la possibilité d'un dialogue de conformité bilatéral au cas par cas avec la CNIL, afin de valider des hypothèses de traitement des données non prévues par le texte.

La loi Informatique et Libertés, modifiée en août 2004, soumet au régime d'autorisation préalable le traitement de données à caractère personnel qui sont susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire. Dans ce cadre, la Commission nationale de l'informatique et des libertés (CNIL), a rendu pour l'année 2005 30 décisions d'autorisation dans le domaine de la lutte contre le blanchiment et le financement du terrorisme. Avant la loi du 6 août 2004, ces dossiers étaient soumis au simple régime de déclaration préalable. Ils nécessitaient le dépôt auprès de la CNIL d'un dossier descriptif composé d'un formulaire et d'annexes qui était soumis à l'étude de la CNIL préalablement à la délivrance du récépissé de déclaration permettant la mise en œuvre du traitement concerné. La décision unique n°AU-003 change la donne pour les organismes financiers. En contrepartie d'un engagement de conformité avec le cadre de référence posé par la décision unique, ils peuvent bénéficier d'une autorisation de mettre en œuvre le traitement sans examen du dossier par la CNIL (contrôle dit a priori). La décision d'autorisation est délivrée immédiatement. La procédure obéit, par conséquent, à la même simplicité que les normes simplifiées de déclaration adoptées par la CNIL pour alléger les formalités des traitements considérés comme les plus courants depuis 1978. Cette nouvelle procédure étant optionnelle, l'organisme financier peut choisir de réaliser une demande d'autorisation plutôt que la décision unique. Le dossier déposé fera alors l'objet d'un examen attentif par la CNIL.

Dans ce contexte complexe, le présent développement ne répondra sans aucun doute pas à l'ensemble des questions soulevées par l'initiative de standardisation prise par la CNIL. L'heure est, en effet, à la compréhension du périmètre de conformité de la décision unique ainsi qu'à ses consé-

quences pour les organismes financiers face à l'obligation de lutte contre le blanchiment et le financement du terrorisme. En substance, le nouveau texte est-il adapté à la réalité opérationnelle ?

LES TRAITEMENTS PERMIS PAR LA CNIL

La décision unique n°AU-003 s'appuie notamment sur les thématiques et l'approche exposées par la CNIL dans un rapport d'étape publié en 2003. La décision devient la partie visible d'un édifice de conformité reposant sur l'ensemble de la loi du 6 août 2004. En résumé, la décision fixe un périmètre de conformité reposant sur sept articles et envisage neuf catégories de situations. Les articles fixent la finalité et le champ d'application des traitements, des données à caractère personnel enregistrées, des destinataires des données, les durées de conservation, les mesures de sécurité, ainsi que l'information à apporter aux personnes concernées. Pour ce qui est des situations, elle envisage de façon méticuleuse neuf domaines qui permettent le traitement de données à caractère personnel. Elle se plie sur ce dernier point à la logique des textes applicables (Code monétaire et financier ou les règlements CRBF). Ces situations concernent la déclaration Tracfin ou le gel des avoirs.

Côté déploiement des systèmes d'information, la décision envisage les traitements répondant à une logique de vigilance administrative, mais semble très restrictive pour ce qui est du recours éventuel à des outils décisionnels. Deux points doivent particulièrement retenir l'attention. Ils posent la question de l'adéquation avec les contraintes réglementaires et opérationnelles des organismes financiers. En premier lieu, la décision couvre uniquement les traitements ayant pour "*finalité exclusive d'apporter une aide à la détection, à l'examen et à la surveillance de certaines transactions financières dans le but éventuel, à l'issue d'une analyse non automatisée*" de réaliser la déclaration Tracfin ou de constituer un dossier de renseignement. Cette précision ferme-t-elle la porte à tout dispositif de profilage ? En second lieu, la décision envisage la possibilité de mettre en place un marquage individuel ("code particulier") des personnes physiques placées sous contrôle interne dans l'hypothèse de fichiers centralisés de la clientèle. La norme étant d'interprétation stricte, le "code particulier" ne devra pas révéler l'existence d'une déclaration de soupçon. En cas de recours à la l'autorisation unique, ces deux points clés de la décision vont nécessiter une analyse juridique préalable de conformité des systèmes d'information existants, et l'adoption d'actions correctives, si nécessaire, pour pallier le risque de non-respect du cadre de la décision unique. En cas de réalisation d'une demande d'autorisation unique complète, ou d'existence d'une formalité réalisée avant la réforme d'août 2004, en dehors du cadre de la décision, quels sont désormais les traitements permis par la CNIL ? La décision unique doit-elle être perçue comme une quasi-recommandation manifestant l'approche générale de la CNIL sur ces sujets ?

INFORMATIONS ET DESTINATAIRES AUTORISÉS

La décision envisage l'enregistrement, le traitement, la production et la transmission d'informations, qui ont vocation à prendre en compte trois fronts opérationnels : celui des clients habituels, des clients occasionnels, mais également des tiers concernés par les opérations financières (donneurs d'ordres, bénéficiaires, personnes politiquement exposées, etc.). La liste des informations est encadrée : identité, situation professionnelle, ainsi que les éléments des opérations financières visées. Les dossiers non automatisés permettraient-ils de traiter d'autres informations ? Autrement dit, ces dernier sont-ils soumis à la décision dès lors que la loi Informatique et libertés modifiée en août 2004 s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers

La décision admet, par ailleurs, une certaine circulation des données. Elles peuvent provenir des services d'un même organisme (agences commerciales, etc.), mais également des services de lutte contre le blanchiment des entreprises d'un même groupe. La décision est en revanche restrictive s'agissant des groupes internationaux. Ce point est évoqué ci-après. Aussi, la norme n'évoque pas la question des informations d'origine GAFI. Côté destinataires, les services internes habilités (lutte contre le blanchiment, contrôle, audit ou juridique) sont clairement des destinataires autorisés, ainsi que les organismes officiels français habituels (Cellule Tracfin du ministère de l'Économie, autorités disciplinaires, direction générale du Trésor).

> *« La décision unique de la CNIL envisage les traitements répondant à une logique de vigilance administrative, mais semble très restrictives pour ce qui est du recours éventuel à des outils décisionnels. »*

ENCADREMENT DES FLUX TRANSFRONTALIERS

La décision unique encadre strictement les flux transfrontières de données, faisant de cette question un chantier de conformité à part entière. Ainsi, la faisabilité d'une communication vers les services de lutte contre le blanchiment d'un même groupe doit être étudiée au cas par cas. Elle nécessite de déterminer si les organismes disposent d'un siège social dans un État membre de la Communauté européenne, d'un État partie à l'accord sur l'espace économique européen, ou dans un État bénéficiant d'un accord bilatéral avec la Commission européenne. Dans ce dernier cas, l'État concerné doit avoir été reconnu par cette dernière comme disposant d'une législation équiva-

lente en matière de protection des données personnelles. La transmission d'informations vers des autorités compétentes situées dans les zones géographiques précitées est également soumise aux mêmes possibilités et restrictions. La décision précise que les destinataires situés hors de France ne pourront pas avoir accès au contenu des déclarations Tracfin et aux suites données à ces dernières. Par ailleurs, plusieurs questions clés liées aux exigences de qualité Informatique et Libertés sont circonscrites dans le périmètre de la décision unique.

En premier lieu, elle fixe une durée de conservation des données différente selon que les traitements d'informations concernent des opérations de lutte contre le blanchiment (5 ans à compter de l'exécution de l'opération litigieuse) ou sur le gel des avoirs (durée des mesures). Qu'en est-il des informations de caractère historique ?

En deuxième lieu, elle pose en obligation l'adoption d'une information explicite des personnes, afin de faire état de l'existence au sein de l'établissement d'un traitement de surveillance. Cette dernière devra être conforme à la loi Informatique modifiée.

En troisième lieu, elle limite les exigences du sacro-saint droit d'accès reconnu aux personnes physiques sur les données les concernant, aux contraintes particulières du sujet traité. La décision précise qu'un organisme financier pourra interroger la CNIL sur le caractère communicable ou non des informations faisant l'objet de la demande. Cette question relève-t-elle de la CNIL ou des autorités ?

En quatrième lieu, la décision rappelle l'importance des mesures de sécurité et de confidentialité Informatique et Libertés en mettant particulièrement en lumière la question des habilitations individuelles. Elle insiste sur l'importance grandissante des politiques de sécurité et de confidentialité Informatique et Libertés comme élément clé d'un dispositif de conformité.

« Quelles options sécurisées s'offrent aux organismes financiers en termes de réalisation des formalités : adhésion à la norme ou dossier complet ? »

DÉCISION UNIQUE OU DOSSIER D'AUTORISATION

Le périmètre de la décision unique étant rappelé, la question peut légitimement se poser de l'applicabilité de la décision unique. Quelles options sécurisées s'offrent aux organismes financiers en termes de réalisation des formalités : adhésion à la norme ou dossier complet ? La décision AU-003 est-elle incontournable ? La CNIL prend position en considérant qu'une autorisation au cas par cas est nécessaire pour les traitements suivants : filtrages utilisant des critères autres que ceux figurant dans l'autorisation unique, tenue des listes de personnes politiquement exposées, gestion ou utilisation de listes d'exclusion de personnes présumées à risques. En fait, deux voies semblent pouvoir être envisagées.

Une première voie pourrait mettre à profit la souplesse de la décision unique vue sous l'angle d'un accord-cadre. Ne posant aucune interdiction, ne couvrant pas l'ensemble des besoins opérationnels, mais se pliant à la lettre des textes applicables, ce dernier est de facto cantonné au rang d'un socle juridique de conformité a minima. Cela pourrait être toute sa force. Ne permet-il pas, en effet, lorsque nécessaire, l'engagement d'un dialogue de conformité bilatéral au cas par cas avec les services de la CNIL, voire tripartite avec les organismes de contrôles, afin de valider des hypothèses de traitements qui, bien que n'entrant pas dans le périmètre étroit de la décision, s'avèrent incontournables pour remplir l'obligation de vigilance. Pour autant, la prise en compte des traitements exclus du périmètre de la norme serait-elle possible ? Selon quelles modalités juridiques ? Il pourrait s'engager une relation inédite apportant aux organismes financiers deux éléments clés : sécurité juridique et souplesse de mise en œuvre. L'ouverture de cette première voie pourrait être facilitée par l'extension inéluctable du périmètre de la décision AU-003 afin de prendre en compte la nouvelle donne résultant de la transposition de la troisième directive européenne.

Une seconde voie, plus classique, consisterait à permettre la réalisation de formalités d'autorisation complètes dès lors qu'un organisme financier constaterait l'inadéquation de la décision unique avec sa situation opérationnelle. Dans l'esprit de la loi Informatique et Libertés modifiée en août 2004, orientée vers une simplification des formalités, cette seconde voie semble difficile d'accès.

UN PLAN DE CONFORMITÉ INFORMATIQUE ET LIBERTÉS

Dans une logique de maîtrise des risques, les organismes financiers doivent engager un plan de conformité Informatique et Libertés. La première étape consistera à établir une cartographie précise des traitements et flux de données, à la constitution d'un inventaire documenté des pratiques existantes et des projets en cours (modes de collecte des informations, analyses décisionnelles, critères de profilage, procédures d'information des personnes, etc.). Ce chantier global de conformité pourra être conduit par un pilote interne en coordination étroite avec les services d'inspection et les déontologue. Certains établissements y trouveront sans doute matière à mettre à profit l'existence d'un *compliance officer* ou d'un correspondant CNIL. La capacité de l'organisme financier à attester sa conformité avec la décision unique est impérieuse. En cohérence avec l'allégement des formalités et l'augmentation de sa capacité de sanction, la CNIL privilégie désormais une démarche de contrôle a posteriori au sein des entreprises. ■