Banques et "vie privée" : problèmes d'application de la loi du 8 décembre 1992

Léonard, Thierry

Published in:
Droit de l'informatique

Publication date:
1993

Document Version
le PDF de l'éditeur

BANQUES ET "VIE PRIVEE": DEUX PROBLEMES D'APPLICATION DE LA LOI DU 8 DECEMBRE 1992

Thierry LEONARD

INTRODUCTION

1. Les banques seront particulièrement attentives aux implications de la nouvelle loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel dans la poursuite de leurs activités(1). La quantité d'informations gérée par les organismes financiers ne cesse de s'accroître. Elle s'explique tant par l'existence d'une très nombreuse clientèle que par la nature des services proposés. Ces derniers impliquent toujours une transfert d'informations du client à la banque; ils demandent bien souvent une connaissance approfondie de la solvabilité des consommateurs.

Le secteur bancaire a très vite compris l'avantage que représentait dans ce cadre une utilisation intensive de l'informatique. Ce niveau d'informatisation élevé lié à la nature particulièrement sensible des informations traitées le met au premier rang des destinataires des législations protectrices de la vie privée. Les banques représentent donc

(1) Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801 et svtes.

un observatoire de choix quant aux difficultés d'application de la nouvelle réglementation.

Si ces difficultés sont nombreuses, elles ne sont pas insurmontables. Elles s'expliquent surtout par le caractère tout à fait général de la loi du 8 décembre 1992 qui ne tient pas compte des spécificités des différents secteurs d'activité. Nous verrons toutefois que la richesse des concepts techniques, à la base de la législation, permet bien souvent de trouver des solutions susceptibles de satisfaire l'ensemble des acteurs.

2. Deux points particuliers retiendront notre attention. Le premier a trait à la détermination des traitements automatisés. De nombreux contacts avec les destinataires de la loi montrent que ces derniers se posent invariablement la même question : que représente, dans la réalité technique qui est la nôtre, la notion de traitement automatisé? Une tentative de réponse émergera d'une analyse de la gestion du fichier "clientèle" détenu par les banques.

Le second vise une difficulté toute particulière rencontrée par le banquier. La gestion des moyens de payement mis à la disposition de sa clientèle lui permettra d'accéder à des informations considérées comme très sensibles par la loi. Ces dernières sont relatives aux opinions politiques, religieuses, syndicales, etc. Elles font l'objet d'un régime de protection spécifique dont la portée se doit d'être clarifiée. Ce problème particulier nous permettra en outre d'affiner notre interprétation de la notion de "traitement automatisé".

CHAPITRE I
LES TRAITEMENTS AUTOMATISES RELATIFS AUX RELATIONS ENTRE LES BANQUES ET LEUR CLIENTELE

3. Le concept de traitement est fondamental dans la compréhension de la nouvelle législation. Premièrement, la portée des obligations mises à charge des organismes bancaires s'en déduit : la loi ne s'applique que si

les données font l'objet d'un traitement(2). Deuxièmement, chaque traitement est à la base de différentes obligations administratives : déclarer *chaque traitement automatisé* auprès de la Commission de protection de la vie privée(3) ; tenir *un état par traitement automatisé*(4) ; transmettre une information à la personne concernée et ce, chaque fois qu'il y a collecte des données auprès d'elle *en vue d'effectuer un traitement* ; informer de la même manière les personnes concernées par les données chaque fois que ces dernières sont enregistrées pour la première fois *dans un de ces traitements*(5) etc.. Tout manquement à ces obligations peut se voir sanctionné au civil comme au pénal. Il est dès lors nécessaire de déterminer le critère qui différencie les traitements entre eux.

4. L'intérêt de la question ressort à suffisance de l'exemple retenu ci-après et relatif à la gestion, par les banques, des données à caractère personnel concernant leurs clients. Dans un premier temps, nous décrirons succinctement la réalité technique mise en oeuvre pour effectuer cette gestion (1.1). Dans un second temps, nous tenterons de déterminer, au regard des exigences légales, les différents types de traitements automatisés de données à caractère personnel qui sont générés par cette réalité technique (1.2). Nous confronterons alors les résultats afin de déterminer si la gestion actuelle des banques est ou non en contradiction avec les exigences de la loi (1.3).

Section 1. La gestion des données "clientèle" : approche pratique

5. La manière dont les grandes banques gèrent l'information relative à leur clientèle constitue le cadre général de notre analyse. Cette gestion

(2) Voir articles 1 §1 et 3 §3 ; aussi Rapport fait au nom de la Commission de la Justice, *Doc. Parl.*, Ch. Repr., sess. extr. 1991-1992, n° 413/12, p. 7 ; pour rappel l'article 1 §1er de la loi précise que l'"on entend par « traitement » le traitement automatisé ou la tenue d'un fichier manuel".
(3) Article 17 §5.
(4) Article 16 §1, 1°.
(5) Article 9.

présente quatre caractéristiques générales(6) dont on peut faire état(7).

La première caractéristique concerne l'utilisation d'une technique fondamentale: l'emploi de réseaux informatiques(8). L'utilisation de réseaux apporte une réponse technique adaptée à l'éclatement de l'informatique en de multiples sites parfois très éloignés les uns des autres. Les réseaux permettent d'interconnecter, grâce à l'utilisation concomitante de l'informatique et des réseaux de télécommunication, une multitude de systèmes isolés en un réseau global.

Le fonctionnement des systèmes informatiques bancaires autour de vastes bases de données de plus en plus centralisées sur un seul site procède de la seconde caractéristique. Ainsi, les terminaux présents dans les agences sont reliés à de grandes bases de données centralisées aux sièges des organismes financiers. Il en résulte par exemple que la modification de l'adresse d'un client à partir du terminal d'une agence est automatiquement enregistrée au niveau des bases de données centrales.

La troisième caractéristique vise le contraste entre la centralisation du stockage et la décentralisation maximale de la collecte(9). De plus en plus, l'encodage des informations s'effectue en une fois en agence et en présence du client lui-même. Cela permet de réduire les risques d'erreurs et de comprimer les coûts d'exploitation. Une fois enregistrée, l'information est stockée au sein de la base de données centrale. Elle ne se retrouve donc qu'à un seul endroit ce qui en facilite grandement la mise à jour et se traduit par un gain de mémoire important.

(6) Remarquons que cette gestion présente des particularités au niveau de chacun des organismes bancaires et que l'on suppose ici un très haut niveau d'informatisation.

(7) Que les informaticiens pardonnent l'auteur... Il ne s'agit pas ici de faire un exposé scientifique et technique concernant les systèmes décrits. Il s'agit ici, modestement, de donner une idée à des non techniciens de la manière dont les outils informatiques sont utilisés de plus en plus fréquemment.

(8) Pour une description plus précise de la manière dont travaillent les banques, voir J.-C. COX, "La loi sur la protection des données à caractère personnel et les réalités opérationnelles des banques - Le point de vue d'un praticien", in *Journée d'étude du 18 mars 1993 - La loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, Association Belge des Banques, à paraître.

(9) Voir pour plus de détails, *Idem*, p. 5 et svtes.

Enfin, dernière caractéristique, le système d'information central est conçu - de manière imagée - comme une armoire munie de différents tiroirs présentant la particularité de s'ouvrir sur d'autres tiroirs (un peu à la manière des poupées russes connues sous le nom de "matrioshka"). Toutefois, l'organisation de cette armoire présente l'immense avantage de permettre des passages directs et rapides entre tiroirs. Ainsi, le tiroir "identification du client" contient les diverses informations nécessaires à son identification ainsi qu'une clé d'accès au tiroir "produit" qui permet la synthèse des relations qu'il entretient avec l'organisme financier (numéros des comptes ouverts, des prêts et crédits octroyés, etc.). A partir de là, il est possible d'accéder à d'autres tiroirs de plus en plus spécialisés en fonction des produits; si le client s'est vu accorder un prêt un tiroir particulier permettra de visualiser le niveau de remboursement, les incidents de paiement, le nombre de lettres de rappel envoyé, etc. On perçoit ici le concept d'intégration de traitements. Les tiroirs sont reliés entre eux par une multitude de liens fonctionnels et informatiques ayant pour conséquence que la modification d'une information au niveau d'un tiroir se répercute dans tous ceux qui ont un lien avec celui-ci. Si le client effectue un remboursement d'une tranche du prêt qui lui est accordé, l'information apparaît au niveau du tiroir "compte" qui indique la débition de celui-ci mais aussi au niveau du tiroir "prêt" qui prend note du remboursement à la date d'échéance.

6. Cette réalité technique a une influence directe sur la manière dont la banque perçoit ses rapports avec sa clientèle. La technique utilisée permet aux institutions d'avoir une vision globale des relations qu'elle entretient avec chacun de ses clients. Elle est donc capable à tout moment d'utiliser la totalité de l'information détenue sur un client "tant pour la gestion des produits dont le client dispose déjà, que pour la vente d'autres produits"(10). Cette vision globale reste-t-elle concevable après la loi du 8 décembre 1992, telle est notre question centrale.

(10) *Idem*, p. 11.

Section 2. La multiplicité des traitements automatisés

1. *La notion de traitement automatisé*

7. L'article 1 § 3 de la loi définit le traitement automatisé comme "tout ensemble d'opérations réalisées en tout ou en partie à l'aide de procédés automatisés et relatif à l'enregistrement et la conservation de données à caractère personnel, ainsi qu'à la modification, l'effacement, la consultation ou la diffusion de ces données".

On sait à quel point l'outil informatique évolue rapidement. Ainsi s'explique la difficulté de cerner dans une définition technique la source du danger nécessitant la protection de l'individu. C'est pourquoi au lieu de dresser une liste des applications susceptibles d'être régies par la loi, le texte appréhende le problème par le biais d'opérations effectuées sur les données. Ce faisant, il se détache de l'outil, de la technique mise en oeuvre pour établir le champ d'application de la protection. Par exemple, l'enregistrement et la conservation de l'identité d'une personne avec son adresse et son numéro de compte peuvent se faire à travers une foule d'outils et de procédés différents (stockage sur la disquette d'un P.C., dans une banque de données, dans un CD-ROM, etc.); cette diversité sera toutefois appréhendée de la même manière par la loi qui y verra un ensemble de données traité en vue de la gestion des comptes. La définition du traitement ne vise donc aucune technique particulière mais bien diverses tâches que ces instruments remplissent(11).

8. La lecture de cette définition conduit à s'interroger sur la manière dont une banque déterminera les différents traitements automatisés poursuivis en vue de gérer ses relations avec sa clientèle. Pourrait-on considérer qu'une banque ne possède qu'un seul traitement "clientèle" englobant l'ensemble des opérations effectuées sur les données concernant celle-ci? Dans le cas contraire, comment distinguer les différents traitements automatisés?

(11) Ainsi pour la C.N.I.L., constitue un traitement un autocommutateur électronique téléphonique, la gestion des badges électroniques, l'usage des cartes à mémoires à microprocesseur incorporé ou à surfaces magnétiques, la messagerie électronique, l'usage d'une machine de traitement de texte pour faire du mailing etc... (voir J. FRAYSSINET, *Informatique, fichiers et libertés: les règles, les sanctions, la doctrine de la C.N.I.L.*, Paris, Litec, 1992, p. 37 spéc. n° 91).

Pour qu'il y ait traitement automatisé, trois conditions doivent être remplies. Tout d'abord, des opérations prévues par la loi doivent être effectuées sur les données; il faut ensuite que ces opérations s'effectuent en tout ou en partie à l'aide de procédés automatisés(12). Ces deux premières conditions ne permettent pas à elles seules de déterminer ce qui dans la réalité correspond à un traitement automatisé. Que des opérations portent sur des données signifie-t-il que l'enregistrement et la conservation de données constituent à eux seuls un traitement automatisé au sens de la loi? Y a-t-il un traitement automatisé lors de chaque modification consécutive de la nature des données traitées? etc. La diversité des procédés automatisés utilisés empêche également de distinguer les traitements automatisés entre eux. Ces procédés se multipliant et s'intégrant tellement les uns aux autres dans le réseau, leur individualisation ne présente aucune utilité.

9. La dernière condition retiendra seule toute notre attention. Pour identifier un traitement automatisé, il faut que les opérations effectuées au moyen de procédés automatisés forment *un ensemble*. Le critère d'unité n'est toutefois pas présent dans la définition même du traitement automatisé. Celui-ci est à trouver dans la finalité poursuivie par celui qui met en oeuvre le traitement.

Le traitement des données poursuit toujours un but déterminé. Les opérations effectuées sur les données s'apprécient en fonction de celui-ci. Elles y trouvent leur raison d'être et leur justification. Si un client ouvre un compte bancaire, il prétend à un service particulier comprenant d'une part la gestion de ses opérations de retraits et de dépôts (en espèces, par virement, chèques, cartes, etc.) et d'autre part la tenue du compte lui-même (mise à jour, fourniture d'extraits, etc.). Pour ce faire, certaines données devront être enregistrées (l'identité, l'adresse, le numéro de compte, la situation matrimoniale, le montant du loyer en cas de virement automatique, etc.), rapprochées (le numéro du compte du donneur d'ordre

(12) Sur ces deux premières conditions voir M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, "La loi du 10 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel", *J.T.*, 1993, à paraître; P. CLAES et J. DUMORTIER, "Privacy-bescherming en gegevensverwerking bij het personeelsbeleid", *Orientatie*, 1, janvier 1993, p. 6.

avec celui du destinataire, les opérations d'achat de carburant sur une période déterminée en cas d'utilisation d'une carte), diffusées (le numéro de compte du donneur d'ordre et la communication seront transmis à la banque du destinataire du transfert de fonds), mises à jour (l'avoir en compte fluctue au gré des opérations) effacées (en cas de clôture du compte), etc. L'ensemble de ces opérations constitue cependant un même traitement automatisé puisqu'elles poursuivent toutes un seul et même but : la gestion des comptes de la clientèle.

10. Le critère de la finalité comme fondement de la détermination du traitement répond parfaitement à la logique de la protection mise en place. De la détermination de la finalité poursuivie découle un grand nombre de conséquences. C'est cette finalité qui permettra de contrôler la légitimité du traitement. Une fois cette finalité déclarée et légitime, les données ne peuvent être utilisées pour d'autres buts. C'est encore en fonction de la finalité du traitement qu'un contrôle des données utilisées est rendu possible; les données doivent en effet être adéquates, pertinentes et non excessives par rapport à la finalité poursuivie. La durée de conservation légitime des données s'apprécie également fonction de la finalité(13).

Bref, la finalité est à la base du système de protection mis en place. En conséquence, chaque finalité implique pour le responsable une attention particulière pouvant se traduire par des solutions différenciées. C'est pourquoi partir du principe que le traitement s'identifie au but qu'il poursuit semble la voie la plus simple pour garantir une protection efficace; une fois les différents traitements déterminés en fonctions des

(13) La durée de conservation des données à caractère personnel est limitée dans la plupart des législations « vie privée » par la reconnaissance d'un droit à l'oubli à l'égard de la personne concernée par les données (voir par exemple l'article 5, e de la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (*Série des Traités européens*, Strasbourg, Janvier 1981, n° 108) qui dispose que les données ne peuvent être conservées que "pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées"). Le législateur n'a pas trouvé bon de rappeler ce principe estimant qu'il découlait directement du principe de finalité ainsi que d'autres dispositions diverses (voir Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445-2, p. 56).

finalités poursuivies, le responsable peut facilement déterminer quelles mesures sont à prendre pour rendre ceux-ci conformes à la loi.

11. Cette conception est unanimement partagée en France(14) où la législation contient une définition du traitement automatisé très proche de la nôtre(15). Ainsi, la C.N.I.L., au terme de dix années d'expériences sur le terrain, précise qu'un traitement automatisé "est un ensemble d'opérations effectuées sur un ensemble d'informations en vue de réaliser une fonction principale déterminée"(16).Cette fonction principale à atteindre est la finalité du traitement, le but d'utilisation des données. On retrouve la même conception aux Pays-Bas où la loi énonce explicitement que le *persoonsregistratie* - concept sui generis qui équivaut à notre notion de traitement - ne peut être mis en oeuvre que pour *un* but déterminé(17).

Le texte de loi belge lui-même semble entériner cette conception. Ainsi, en cas de collecte de données effectuée en vue d'*un* traitement, la personne concernée doit être informée de *la* finalité pour laquelle les données seront utilisées; elle a également le droit d'obtenir la suppression ou l'interdiction d'utilisation de toute donnée la concernant qui, compte

(14) Consulter sur ce point J. FRAYSSINET, *op. cit.*, p. 36 et suivantes; voir aussi les normes simplifiées de la C.N.I.L. qui définissent leur champ d'application relativement aux finalités poursuivies par les traitements (pour consulter celles-ci voir *J.O.*, brochure INFORMATIQUE ET LIBERTES n° 1473, éd. juillet 1991).

(15) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.*, 7 et rectif. 25 janv. 1978; voir l'article 5 qui définit le traitement automatisé comme : "tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment, les interconnexions ou rapprochements, consultations ou communications d'informations nominatives".

(16) CNIL, *Dix ans d'informatique et libertés*, Paris, Economica, 1988, p. 51.

(17) Article 4.1 de la loi néerlandaise (Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levensfeer in verband met persoonsregistraties, *Staatsblad*, 1988, 665); voir aussi les articles 4.2. et 5 qui parlent toujours du persoonsregistratie par rapport à une finalité; voir sur ce point J. DE BAKKER, J. HOLVAST, R. KETELAAR, *Wet persoonsregistratie - Een praktische handleiding*, Amsterdam, Stichting Waakzaamheid Persoonregistratie, 1990, p. 60 où les auteurs donnent des conseils pratiques aux destinataires de la loi afin de déterminer une finalité par *registratie*.

tenu *du but du traitement*, est incomplète ou non pertinente(18); le maître du fichier est tenu d'établir, pour chaque traitement, un état où est notamment consigné *le but du traitement*(19); il doit également mentionné dans la déclaration de chaque traitement automatisé *le but poursuivi* par celui-ci(20).

12. Cette conception du traitement automatisé présente un immense avantage: la loi devient totalement indépendante de l'évolution technologique. Par le biais d'un concept abstrait, la loi instaure un cadre dans lequel la technique va pouvoir évoluer(21). Que l'on se trouve en présence d'un large réseau informatique où plusieurs ordinateurs localisés en des lieux différents s'intègrent dans un système unique, de nouvelles technologies de l'information utilisant les richesses de la télématique, d'un P.C. portable ou de tout autre procédé automatisé, la logique de protection est identique. Une seule question se pose: dans quel but utilise-t-on les données à caractère personnel?

B. La détermination des finalités

§ 1. Approche théorique

13. La notion de finalité n'est pas éclaircie pour autant. Chaque opération portant sur les données ayant une utilité bien précise (les enregistrer, les modifier, les rapprocher, etc.), on pourrait conclure à

(18) Article 12 §1 al. 2.

(19) Article 16 §1, 1°.

(20) La rédaction de l'article 5 pourrait toutefois contredire *a priori* notre interprétation ("Les données à caractère personnel ne peuvent faire l'objet d'*un* traitement que pour *des* finalités déterminées et légitimes (...)"). Elle laisse entendre qu'un traitement pourrait poursuivre diverses finalités distinctes. A la réflexion, nous pensons qu'il n'en est rien. La version française de l'article 5 doit être ici éclairée tant par le reste du texte que par sa version néerlandaise. Cette dernière est rédigée un peu différemment ("Persoonsgegevens mogen slechts *worden verwerkt* voor duidelijk omgeschreven en wettige doeleinden (...)"). Ce faisant, elle met l'accent sur la seule leçon que l'on puisse tirer de cet article concernant la notion même de traitement: les mêmes données peuvent être traitées pour des finalités différentes, mais ces dernières doivent être déterminées et légitimes.

(21) Dans le même sens voir Rapport fait au nom de la Commission de la Justice, *Doc. Parl.*, Sén., sess. extr. 1991-1992, n° 445/2, p. 19; voir aussi J. FRAYSSINET, *op. cit.*, p. 36, n° 87 et svts.

l'existence d'un traitement par opération. Cette vision aurait des conséquences absurdes qui rendraient vite le système ingérable; il faudrait par exemple déclarer chaque opération... Il faut donc remonter la chaîne afin de regrouper entre elles les opérations qui offrent un lien suffisamment étroit pour présenter une certaine unité. C'est toute la difficulté de la recherche des finalités.

Cette recherche devrait, selon nous, s'effectuer au regard du principe fondamental de la protection mise en place par la loi: le principe de finalité. Pour être bien compris, il est nécessaire d'en rappeler les grandes lignes.

a) Le principe de finalité

14. L'article 5 de la loi détermine le principe de finalité en ces termes: "Les données à caractère personnel ne peuvent faire l'objet d'un traitement que pour des finalités déterminées et légitimes et ne peuvent pas être utilisées de manière incompatibles avec ces finalités; elles doivent être adéquates, pertinentes et non excessives par rapport à ces finalités"(22).

Cette disposition énonce deux principes distincts(23). Le premier - principe de légitimité - postule que le but du traitement soit déclaré et légitime. Le second - principe de conformité - exige un lien étroit entre les données utilisées et la finalité légitime déclarée. Toute utilisation des données doit être compatible avec la finalité. Plus précisément, les données doivent être adéquates, pertinentes et non excessives par rapport à cette finalité.

15. Le principe de légitimité obéit lui-même à deux règles. La première, formelle, exige que le but poursuivi par le traitement soit déterminé. Elle est au fondement d'une exigence de *transparence* des circuits

(22) Remarquons que c'est la première fois que ce principe est consacré dans une législation nationale de manière aussi explicite.

(23) Sur ces distinctions v. Th. LEONARD et Y. POULLET, "Les libertés comme fondement de la protection des données nominatives", in F. RIGAUX, *La vie privée une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur n° 17, Bruxelles, Larcier, 1992, p. 232 et svtes, spéc. n° 35 et svts.

d'information à l'égard de l'individu qui sous-tend l'ensemble du texte de loi. La poursuite d'une finalité secrète ou imprécise est donc exclue. Cette première exigence - abstraite - de transparence se traduit par diverses obligations concrètes mises à charge du responsable du traitement. Ces obligations visent à informer d'une part les individus de l'existence de traitements portant sur les données qui les concernent(24) et d'autre part la Commission de la vie privée chargée du contrôle de la mise en oeuvre de ces traitements(25). Elles permettront aux personnes concernées d'exercer les droits qui leur sont reconnus (droit d'accès et de rectification). La Commission y trouvera les éléments lui permettant de prendre toute mesure propre à garantir la bonne application de la loi (demande de compléments d'informations, descente sur les lieux et.). Dans ces deux hypothèses, l'information comprend notamment la description de la finalité pour laquelle les données recueillies seront utilisées.

16. La seconde règle a trait à l'objet même de la finalité. Celle-ci doit être légitime. Il est curieux que cette exigence n'ait été précisée nulle part. Certes, la finalité du traitement ne peut être contraire à l'ordre public et aux bonnes moeurs. La philosophie de la loi invite cependant à une interprétation téléologique du principe de légitimité. Si le but est bien de garantir la protection de la vie privée des individus dans notre société, la finalité du traitement et sa mise en oeuvre doivent concilier les intérêts de la personne concernée par les données et l'intérêt général ou l'intérêt particulier poursuivi par le responsable du traitement. La légitimité implique donc un équilibre entre les différents intérêts qui s'opposent. Il en résulte qu'une finalité choisie violant les intérêts individuels sans se fonder sur un intérêt supérieur doit être considérée comme illégitime. Imaginons par exemple l'Etat mettre sur pied un traitement relatif aux habitudes sexuelles de sa population sous prétexte de déterminer les personnes "à risque" concernant la transmission du S.I.D.A.. Une finalité serait de même illégitime, selon nous, si la poursuite de l'intérêt du ficheur implique pour l'individu des risques disproportionnés par rapport à ce qui est strictement nécessaire. Une banque a ainsi intérêt à mettre sur

(24) Article 4 §1 et article 9.
(25) Article 17 et 18.

pied un traitement automatisé à finalité de marketing; elle devrait toutefois laisser la possibilité au client de refuser l'envoi de mailings et autres publicités. La Commission de protection de la vie privée et le juge contrôleront cette légitimité sur base de la méthode de pondération des intérêts, reposant sur la règle de proportionnalité(26).

17. Une finalité légitime et déclarée n'autorise pas d'elle-même l'utilisation de n'importe quelle donnée. Le principe de conformité implique tout d'abord que l'utilisation des données soit compatible avec la finalité légitime et déclarée. Si une entreprise déclare traiter des données en vue de la gestion de son fichier clientèle, cela ne lui permet pas automatiquement de les vendre à une autre entreprise. Pour ce faire, elle devrait déclarer cette autre finalité dont la légitimité serait contrôlée.

Le principe de conformité implique également que les données utilisées soient adéquates, pertinentes et non excessives par rapport à la finalité déclarée et légitime. On retrouve ici explicitement la règle de proportionnalité. L'adéquation et la pertinence de la donnée ne visent rien d'autre qu'une liaison nécessaire et suffisante de l'information au but poursuivi par le traitement. Pour gérer le compte d'un client adulte une banque n'a pas besoin de prendre en compte le montant des revenus professionnels des parents. Le caractère non excessif de la donnée exige que son utilisation soit écartée si elle présente un risque d'atteinte disproportionné par rapport aux intérêts individuels de la personne concernée. Ainsi, les données déduites des mouvements en compte d'un client - par exemple le montant des primes d'assurance payées par le client - ne pourraient servir à la banque pour faire une offre alléchante concernant ses propres produits d'assurance.

b) Les deux principes de détermination des finalités

18. Que le principe de finalité guide la détermination des finalités elles-mêmes pourrait surprendre. Le contrôle de la correcte application des deux principes qui en découlent - légitimité et conformité - suppose que

(26) Sur la méthode de contrôle préconisée voir Th. LEONARD et Y. POULLET, *op. cit.*, n° 28 et svts.

la finalité soit préalablement circonscrite avec précision. Cette affirmation vaut pour les organes de contrôle qui interviennent en aval de la détermination des finalités. La position du maître du fichier désireux de se conformer à la loi est différente. C'est à lui qu'il revient, avant tout autre, de déterminer les finalités qu'il poursuit ou s'apprête à poursuivre. Pour ce faire, rien ne s'oppose à ce qu'il soit guidé par les implications du principe de finalité.

19. Comment va procéder le maître du fichier pour déterminer les finalités des différents traitements qu'il met en oeuvre?

Le maître du fichier doit d'abord mettre en avant les raisons qui le poussent à stocker ou utiliser des données à caractère personnel. Il traite ces dernières selon le cas pour gérer ses relations avec sa clientèle ou son personnel, pour mettre en oeuvre une campagne publicitaire ou plus simplement pour gérer le service qu'il rend... Tout cela est encore bien flou mais suffisant pour démarrer; c'est la première étape.

Le maître du fichier peut également percevoir facilement que la plupart des règles de la loi présentent un lien direct avec la finalité d'utilisation des données. Or, seul l'article 5 s'attache à déterminer tant la qualité de la finalité (légitime et déclarée) que ses exigences immédiates en ce qui concerne la protection mise en place (conformité des données). En effectuant quelques recherches, le maître du fichier connaîtra également la portée précise de cette disposition. Ce faisant, il franchit la seconde étape.

Il terminera en confrontant les buts d'utilisation qu'il perçoit intuitivement aux exigences du principes de finalité. Ce dernier lui fournira les outils nécessaires. Ce faisant, il parviendra petit à petit à cerner les finalités d'utilisations qu'il poursuit et partant le nombre de traitements automatisés qu'il met en oeuvre.

20. Deux critères de sélection permettront au maître du fichier d'affiner ses intuitions de départ: l'exigence de transparence et les règles de fond du principe de finalité.

La finalité poursuivie par le traitement automatisé doit être déterminée. Cela suppose qu'elle soit suffisamment précise pour que les

destinataires de l'information puissent correctement remplir leur rôle dans le système de protection. La personne concernée ne saurait contrôler utilement les données si elle ne connaît pas précisément les différentes utilisations qui en sont faites. Le même raisonnement peut être tenu en ce qui concerne la Commission. Deux conséquences en résultent. Tout d'abord, les finalités trop générales sont à exclure; elles ne permettent aucun contrôle. Ensuite, la finalité déterminée ne peut couvrir que des utilisations de données apparaissant aux organes de contrôle et à la personne concernée comme des implications "normales" de celle-ci.

La règle de fond du principe de légitimité ainsi que le principe de conformité permettront également d'aider le maître du fichier. La finalité retenue doit rencontrer leurs exigences. Si elle masque des sous-finalités présentant des divergences dans le contrôle de légitimité et de conformité, elle doit être rejetée. La finalité gestion du personnel peut englober différents traitements automatisés ayant des finalités incompatibles; la gestion des payes et le contrôle des déplacements dans l'entreprise par exemple. La légitimité et la conformité des données utilisées posent dans ces hypothèses des problèmes totalement différents qui se marquent tant au niveau des catégories de données utilisées que des risques engendrées par leur traitement. Il doit donc y voir deux traitements différents.

21. Est-ce à dire que toute finalité « générique » est à proscrire? Toute application ne constitue pas un traitement automatisé. Pensons à la gestion des comptes bancaires. Les opérations tendant à l'enregistrement et la mise à jour des données relatives à l'identification du titulaire du compte ne divergent pas fondamentalement de celles permettant la mise à jour de l'avoir en compte. Ces opérations ne génèrent pas une finalité différente de celle, générique, visant à la "gestion des comptes". Elles s'induisent de cette dernière sans demander une attention particulière en ce qui concerne leur légitimité ou la conformité des données utilisées. Les différentes utilisations des données sont conformes à l'attente du client: la gestion du compte qu'il a ouvert auprès de l'institution qui traite les données. La situation serait différente si certaines de ces données étaient cédées à des tiers - des grandes surfaces par exemple - afin de déterminer les habitudes de consommation du titulaire du compte.

On peut donc en conclure qu'une finalité générique est acceptable dès lors que toute utilisation des données qui en découle y est conforme

tant du point de vue de la transparence que des exigences du principe de finalité. L'article 5 de la loi contient expressément cette solution lorsqu'il énonce que les données ne peuvent être utilisées de manière incompatibles avec les finalités légitimes et déclarées(27).

§ 2. Application au fichier "clientèle" de la banque(28)

22. Loin de nous l'idée de soutenir que le modèle avancé ici constitue l'unique réponse à la question de savoir quels traitements automatisés sont mis en oeuvre dans les relations des banques avec leur clientèle. L'important est plutôt de montrer comment les critères de déterminations des finalités peuvent guider dans la pratique le maître du fichier qui tente de se conformer à la loi du 8 décembre 1992.

23. Dans quels buts une banque utilise-t-elle les données à caractère personnel concernant sa clientèle? Principalement pour gérer les produits qu'elle lui offre. De cette constatation découle une première distinction entre les différentes utilisations des données; la gestion des produits offerts ne peut se confondre avec une utilisation des données visant à cibler le plus précisément les personnes susceptibles d'être intéressées par ces produits, tout en présentant des garanties de solvabilité suffisantes pour y faire face. Le principe de transparence fonde cette première distinction. Pour le client, comme pour les autorités de contrôle, la *finalité «marketing»* présente des implications différentes de celle *«gestion des produits»*. La finalité marketing ne se déduit pas nécessairement de la gestion du compte qu'il ouvre auprès de l'organisme ou du prêt qu'il se voit octroyer; le marketing présente en termes de légitimité et de conformité des donnés un régime différent de la gestion des produits.

Intuitivement, on perçoit en outre une troisième finalité tout à fait générale poursuivie par la banque. Dans différentes hypothèses, celle-ci

(27) Voir aussi l'article 6.1 de la loi néerlandaise qui énonce que (trad.) "les données à caractère personnel rassemblées ne peuvent être utilisées que dans des buts compatibles avec celui du *persoonsregistratie*" ("De opgenomen persoonsgegevens worden slechts gebruikt voor doeleinden die met het doel van de persoonsregistratie verenigbaar zijn").

(28) On utilise ici la notion de fichier au sens le plus classique du terme: l'ensemble des données traitées relatives à la clientèle.

transmettra des données à des tiers sans que la communication ne participe directement à une des deux autres finalités. Pensons par exemple aux données obligatoirement transmises à la centrale négative tenue par la Banque nationale de Belgique. Le client, même s'il est conscient des difficultés qu'il rencontre lors du remboursement d'un crédit qui lui a été octroyé, ne peut en déduire implicitement qu'il acquiert par ce fait l'image d'un "mauvais payeur" qui sera diffusée au sein de la profession. Le principe de transparence implique donc que cette finalité soit mise en exergue. Cela permettra d'ailleurs au consommateur de prendre conscience des risques qu'il encourt mais aussi de contrôler l'usage des données qui le concernent ainsi que la qualité de l'information qui circule à son propos.

a) La gestion des produits

24. La "gestion des produits" est-elle une finalité suffisamment déterminée permettant de satisfaire les exigences de fond du principe de finalité et de transparence?

Le principe de transparence semble *a priori* respecté. On peut en effet raisonnablement penser que le client connaît les produits bancaires qu'il utilise. Différencier les finalités de gestion par produit (compte à vue, compte épargne, accès au réseau bancontact, etc.) ne paraît pas utile sur ce point.

Toutefois, le principe de finalité oblige à affiner l'analyse. Certains groupes de produits impliquent en eux-mêmes un besoin d'informations plus grand que d'autres. Les banques se voient en effet dans l'obligation d'avoir une idée pleine et entière de la solvabilité du client demandeur de certains produits. C'est tellement vrai que la responsabilité du banquier peut se voir engagée au cas où il n'a pas mis tout moyen en oeuvre pour évaluer la capacité de remboursement du client. Nous pensons ici, de manière générale, aux crédits et prêts que les banques octroient à leur clientèle.

25. Dès lors, apparaît selon nous une nouvelle finalité que l'on dénommera *gestion des produits à risques*. Cette finalité se doit d'être indépendante des autres finalités de gestion des produits; sa poursuite implique l'accès à un grand nombre d'informations dont la conformité au

but poursuivi s'appréhende de manière spécifique. Le problème n'est pas seulement de déterminer les données nécessaires au suivi du service rendu ; la gestion des prêts et crédits implique qu'au départ une décision soit prise en fonction des risques de non-remboursement présentés par un individu spécifique. L'analyse de l'adéquation, de la pertinence et du caractère non excessif des données se fera par rapport à cette analyse de solvabilité. Ces données pourront servir également à fonder une décision sur les moyens qui, le cas échéant, seront mis en oeuvre aux fins de récupération des sommes prêtées. La transparence s'en trouve également renforcée ; le client sera informé non seulement de la nature particulière de cette finalité mais aussi des catégories de données nécessaires à sa poursuite. Il pourra alors plus facilement apprécier leur conformité par rapport à celle-ci.

Pour être parfaitement transparent, on pourrait conseiller aux organismes bancaires de préciser en sus de la finalité particulière - gestion des produits à risques - diverses sous-finalités qui, quoique participant toutes au même but, permettent d'apprécier avec un maximum de précision les limites de l'utilisation des données. La première pourrait consister en l'analyse de la solvabilité du client en ce compris l'utilisation des techniques de "crédit-scoring". La seconde engloberait toutes les opérations propres à la gestion du crédit ou du prêt consenti en ce compris la gestion d'un éventuel contentieux. Ces sous-finalités ne rélèvent pas à notre sens de traitements particuliers(29) ; elles s'inscrivent très exactement dans la relation poursuivie par le client. Il se peut toutefois que certaines applications tendant à l'évaluation de la solvabilité fassent l'objet d'une réglementation particulière. Elles constitueront alors des traitements spécifiques.

26. Cette finalité particulière de *gestion des produits à risques* s'opposera à la *gestion des produits sans risques*. Ces derniers visent globalement l'ensemble des placements de la clientèle ainsi que la gestion de services qui lui sont rendus. Ces sous-finalités ont toutes en commun de n'impliquer qu'une demande d'informations banales orientée vers la fonctionnalité des services. Le nom, l'adresse, le numéro de compte, les moyens de paiement utilisés, etc. seront ainsi nécessaires à la tenue du

(29) Sous réserve de ce qu'il sera dit concernant la vision globale (cf. infra Section 3.).

compte, l'élaboration des extraits, etc. Il ne s'agit plus ici pour la banque de prendre des risques particuliers vis-à-vis de la clientèle mais bien à la fois d'attirer des capitaux afin de les rémunérer (comptes-épargnes, bons de caisse, etc.), et gérer les transferts de fond effectués par ou au profit des titulaires de comptes ouverts dans l'établissement.

27. Remarquons cependant que l'utilisation des produits - qu'ils soient à risques ou sans risques - va parfois produire de nouvelles informations qui pourraient être utiles au banquier. Ainsi, les transferts électroniques de fonds constituent la source d'une foule d'informations(30) : l'utilisation du guichet automatique de banque permet de connaître non seulement l'identité de l'utilisateur mais aussi le lieu et l'heure de la manipulation ; l'utilisation d'un terminal point de vente renseigne l'organisme financier sur l'identité du commerçant, l'importance et le moment de la transaction, voire sa nature. De plus, la technique rend possible l'analyse de ces informations afin d'en retirer d'autres comme l'image précise des habitudes de consommation d'un client, de ses déplacements, de la manière dont il utilise les services mis à sa disposition, etc. Il y a ici trois niveaux d'informations : les informations rassemblées en amont de l'utilisation du service (identité du client, numéro de compte, etc.) ; celles qui apparaissent lors de l'utilisation du service (montant des transactions, lieu, moment, identité du bénéficiaire, etc.) ; celles qui constituent le résultat de traitements des informations des deux autres niveaux (habitudes de consommation, de déplacement, etc.). Comment ces niveaux d'informations s'intègrent-ils dans notre modèle ?

Les données des deux premiers niveaux sont traitées en vue de la seule gestion du produit offert. Dès lors que seules les données nécessaires à la fourniture et à la gestion du service sont enregistrées et

(30) Voir sur ce point Y. POULLET, "T.E.F. et protection des données à caractère personnel", in *Transfert électronique de fonds et protection du consommateur*, Bruxelles, Story Scientia, Collection droit et consommation, 1990, spéc. p. 181 à 183.

utilisées(31), elles font l'objet d'une ou l'autre des finalités déterminées ci-avant. On retrouve là le principe de conformité tel qu'explicité plus haut. Seul le troisième niveau d'informations découle de traitement distincts de ceux repris jusqu'à présent dans notre modèle. Il ne s'agit plus ici de s'en tenir à ce qui est nécessaire aux fins de la gestion du service. La finalité est alors différente et les opérations portant sur les données participent à un traitement distinct soumis spécifiquement aux exigences du principe de finalité.

28. A notre sens une dernière finalité doit être distinguée au niveau de la gestion des produits. Dans différentes hypothèses, le service offert par la banque consiste en une aide à la gestion du patrimoine de la clientèle. On pense par exemple aux simulations permettant au client de calculer le montant de ses impôts ou la charge d'un financement éventuel. La gestion de tels services implique également un besoin important d'informations. Dans le premier exemple précité, la banque doit collecter et traiter l'ensemble des informations nécessaires au calcul de l'impôt représentant presque la totalité des avoirs de l'individu. Elle pourrait trouver là une source nouvelle d'informations non conforme aux finalités mises précédemment en avant. Ce type de traitement paraît de plus présenter des risques particuliers de réutilisation de l'information pour des buts totalement étrangers à la finalité de départ. On doit donc y voir un troisième traitement mis en place au niveau de la gestion des produits.

(31) Voir dans le même sens la Recommandation n° R (90)19 du Comité des ministres aux Etats membres du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins de payement et autres opérations connexes du 13 septembre 1990; celle-ci distingue les données à caractère personnel liées à la fourniture ou à l'utilisation des moyens de payement (art. 2). On retrouve là nos deux premiers niveaux d'information. Les données liées à la fourniture du service ne peuvent être collectées et enregistrées que si elles paraissent nécessaires pour la mise à disposition du moyen de payement et son contrôle (art.3.1.) Les données liées à l'utilisation du moyen de payement ne peuvent être enregistrées que dans la mesures où elles sont nécessaires à la validité et à la preuve de l'opération ainsi qu'à la réalisation des services et à la prise en compte de toute obligation découlant du droit interne liée à son utilisation (art. 3.5).

b) Le marketing direct

1° - Généralités

29. On peut définir le marketing direct comme "l'ensemble des activités ainsi que tout service auxiliaire à celles-ci permettant d'offrir des produits et des services ou de transmettre tous autres messages publicitaires à des segments de population par le moyen du courrier, du téléphone ou d'autres moyens directs dans le but d'information ou afin de solliciter une réaction de la part de la personne concernée"(32).

Contrairement à la publicité classique qui s'adresse à tous par voie d'affichage, de spots télévisés, etc., le marketing direct vise à instaurer un dialogue direct entre partenaires; il s'agit d'interpeller personnellement le consommateur afin de susciter une réaction rapide de sa part(33). Généralement un imprimé sera envoyé au domicile de l'individu ou encore au lieu où il exerce son activité professionnelle. Les nouvelles technologies de télécommunication ont encore facilité la prise de contact directe avec le consommateur. Ainsi, le démarchage par téléphone - éventuellement par le biais d'un automate d'appel - ou par télécopie devient de plus en plus fréquent(34).

30. Le marketing direct nécessite l'utilisation de listes d'adresse mises à jour et différenciées selon le type de produit. Celles-ci ne sont toutefois pas suffisantes. Un marketing direct efficace implique que les consommateurs, destinataires du message publicitaire, soient soigneusement ciblés en fonction de caractéristiques qui leur sont propres (niveau de revenus, catégorie socio-professionnelle, lieu d'habitation,

(32) Article 1.2. de la Recommandation n° R (85) 20 adoptée par le Comité des ministres du Conseil de l'Europe le 25 octobre 1985 et relative à la protection des données à caractère personnel utilisées à des fins de marketing direct.

(33) Pour plus de détails, voir J.-P. WALTER, "Recommandation n° R (85) 20 du Comité des ministres du Conseil de l'Europe relative à la protection des données à caractère personnel utilisées à des fins de marketing direct", in *XIIIème Conférence des Commissaires à la Protection des données (2-4 octobre 1991)*, Conseil de l'Europe, Strasbourg, 1992, p. 128 et 129.

(34) Sur ce problème spécifique voir H. BOUCHET, "Nouvelles techniques de marketing direct et législation sur la protection des données", in *XIIIème Conférence des Commissaires à la Protection des données (2-4 octobre 1991)*, Conseil de l'Europe, Strasbourg, 1992, p. 149 à 156.

etc.). Deux étapes sont à distinguer lors d'une campagne de marketing. La première consiste à rassembler un maximum de données à caractère personnel relatives à une population particulière. La seconde vise à sélectionner les individus dont le profil permet de penser qu'ils seront plus que d'autres intéressés par le produit ou le service proposé, tout en présentant des garanties financières suffisantes pour faire face aux coûts d'acquisition(35). L'utilisation de ces techniques permettra non seulement une réduction des coûts mais aussi des risques pour le commanditaire de la campagne de publicité.

31. Les traitements de données à caractère personnel nécessaires à la constitution de listes d'adresse aux fins de marketing direct posent des problèmes spécifiques au regard de la protection de la vie privée des personnes concernées par les données. Les principales difficultés peuvent être résumées comme suit :

1) Le démarchage publicitaire direct des particuliers importune parfois les destinataires qui peuvent éprouver le besoin d'être laissés tranquilles(36) ;

2) Ce sentiment d'irritation est d'autant plus important que le destinataire ne comprend pas comment son adresse est en possession de

(35) Voir la distinction entre la "liste de marketing direct" et le "fichier de marketing" telle que retenue par la Recommandation n° R (85) 20 du Conseil de L'Europe (*op. cit.*). Le premier terme vise "toute collection de noms et d'adresses, y compris les informations se limitant à l'indication de l'intérêt éventuel du consommateur ou du donateur, utilisée pour communiquer avec les personnes concernées". Le second a trait à "toute collection de données à caractère personnel ou d'autres données, dans la mesure où celles-ci sont collectées et utilisées pour établir des listes de marketing direct" (Exposé des motifs, p. 14, n° 11). La recommandation réglemente principalement les listes de marketing direct sans apporter une réponse satisfaisante aux problèmes spécifiques à la mise en oeuvre des fichiers de marketing. Pour une critique de cette approche, voir J.-P. WALTER, *op. cit.*, p. 147 et 148.

(36) Voir par exemple pour une analyse nuancée de cette irritation, P.L.C. NELISSEN, "Brievenbusreclame gooi ik altijd ongelezen weg ; alleen wat ik interessant vind, bewaar ik", *Privacy en Registratie*, 1991/2, p. 14 à 17 ; voir pour un exemple caractéristique de "harcèlement téléphonique" CNIL, *11ème rapport d'activités-1990*, Paris, Doc. Fr., 1991, p. 36.

la société qui lui offre ses produits ou services(37). De manière générale, le manque de transparence des circuits d'informations est à la base de la création des législations protectrices de la vie privée. Il se pose toutefois de manière accrue dans une activité qui se fonde sur un échange et une interconnexion généralisés de données à caractère personnel ;

3) La création des listes d'adresses suppose la constitution de profils précis des consommateurs. Or, comme le rappelait le professeur Rigaux dans un article récent, les profils peuvent paraître incompatibles avec la liberté de la vie privée car "ils attribuent à une personne individuelle les modes de comportement ou de consommation du groupe auquel elle appartient. Impliquant que le sujet est prédéterminé par son appartenance à un groupe, ils sont négateurs de la liberté individuelle : cette liberté est gravement atteinte si un doute est jeté sur l'aptitude d'une personne à améliorer son comportement, quelque chargés que soient son passé ou son environnement social"(38) ;

4) L'application du principe de finalité soulève des difficultés particulières. Si la légitimité des traitements poursuivis ne peut être niée endéans le respect de certaines règles protectrices, la détermination des finalités risque d'être délicate. Pourra-t-on se contenter d'une seule finalité générique "marketing direct" ou répertorier autant de finalités que de campagnes publicitaires à lancer ? Il est clair que l'information nécessaire variera de manière substantielle en fonction du produit en cause. La promotion d'un compte courant spécifique pour les "jeunes" ne génère pas le même besoin de données à caractère personnel que celle d'un nouveau type de crédit hypothécaire. Faut-il y voir la création de deux traitements automatisés différents avec toute la charge administrative que cela suppose ? La mise en oeuvre du principe de conformité pose également problème. Le ciblage se fondant généralement sur des analyses statistiques préalables, le contrôle du caractère adéquat, pertinent et non excessif de la donnée n'implique-t-il pas un contrôle du caractère objectif

(37) Qui n'a pas remarqué que le simple fait de débuter une carrière professionnelle se traduit par un engorgement quasi immédiat de sa boîte aux lettres ?

(38) F. RIGAUX, "La protection de la vie privée à l'égard des données à caractère personnel", *Annales de droit de Louvain*, 1993/1, p. 64, n° 17.

du raisonnement qui sous-tend la mise en profil de l'individu(39) ? Dans le cas contraire, comment apprécier l'utilité et la nécessité de la donnée ?

5) Par ailleurs, une attention particulière doit être portée au principe de loyauté de la collecte(40). Pensons par exemple à certaines méthodes de marketing actifs où les réactions de la personne contactée par téléphone sont analysées par ordinateur afin d'en tirer des informations concernant la psychologie de l'individu. Citons également le dépouillement systématique des ordres de virement d'un individu en vue de l'élaboration de son profil de consommation.

32. Malgré ces difficultés particulières, la légitimité des traitements utilisés à des buts de marketing direct n'a jamais été niée. Le marketing direct représente aujourd'hui une réalité économique incontournable. Les données à caractère personnel - qui constituent la matière première indispensable à cette activité - ne sont toutefois pas des biens de consommation comme les autres. C'est pourquoi le droit doit prévoir des garanties particulières propres à sauvegarder les libertés individuelles des personnes concernées. Celles-ci ne sont présentes que très partiellement dans les législations générales du type de la loi du 8 décembre 1992.

On constate aujourd'hui l'émergence de principes de protection particuliers issus tant de réglementations sectorielles, que de pratiques prônées par les organes de contrôle ou de codes de conduites adoptés par le secteur du marketing lui-même. L'analyse systématique de ceux-ci sortirait largement du cadre limité de cette analyse. Nous nous contenterons ici de déterminer les principes propres à guider une banque lors de l'utilisation des données issues de son fichier clientèle en vue de finalités de marketing.

(39) L'article 3 de la loi française, contrairement à la loi belge, prévoit d'ailleurs explicitement que "toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés"; voir Th. LEONARD et Y. POULLET, *op. cit.*, p. 246 n° 20; concernant l'utilisation du crédit-scoring, voir P. DEJEMEPPE, "La mémoire de l'argent. La protection des données à caractère personnel dans la loi du 12 juin 1991 relative au crédit à la consommation", *D.C.C.R.*, Janvier 1992, n° 14, p. 895 et svtes.

(40) Qui est étrangement absent de la loi du 8 décembre 1992.

2° - L'utilisation du fichier clientèle à des fins de marketing direct

33. De par la nature et la diversité des produits offerts, la banque dispose d'un fichier marketing d'une remarquable richesse. Les données financières directes (avoirs en compte, crédits octroyés, etc.) liées à celles provenant de l'analyse de la solvabilité (revenus professionnelles, avoirs du ménage, etc.) voire de l'utilisation des moyens de payement (habitudes de consommation, goûts personnels, etc.) permettent la constitution de profils très précis de la clientèle. Ce fichier de marketing, encore enrichi par rapprochement avec d'autres fichiers extérieurs(41), donne à la banque la possibilité de déterminer avec un maximum de précision les clients à démarcher lors d'une campagne promotionnelle.

- *La légitimité*

34. L'utilisation du fichier clientèle d'une banque en vue d'effectuer du marketing direct ne pose pas de problème si certaines conditions sont remplies. L'exposé des motifs de la loi du 8 décembre 1992 est parfaitement clair à ce sujet(42). Comme le rappelait récemment la C.N.I.L., "dans le cadre de son activité, il paraît normal qu'une société utilise les informations en sa possession pour adapter ses propositions commerciales aux différents types de clientèle"(43).

(41) Voir les craintes de la C.N.I.L. vis-à-vis des rapprochements entre fichiers clientèle des banques et ceux de sociétés spécialisées dans le traitement automatisé ayant pour finalité la réalisation et la fourniture de sélections de population établies en fonction de données géographiques et socio-économiques (CNIL, *11ème rapport d'activités-1990*, Paris, Doc. Fr., 1991, p. 101).

(42) Il y est précisé que "Le présent article (*ndlr anc. article 6 - article 5 nouveau*) ne vise pas à empêcher que des données soient utilisées pour répondre à des finalités multiples pour autant que celles-ci soient clairement précisées dès l'origine. Ainsi par exemple une firme privée pourrait être amenée à enregistrer des données relatives à sa clientèle à la fois pour la gestion des relations qu'elle entretient avec les clients (suivi des commandes, facturation etc...) et pour de nouvelles prospections" (Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. Parl.*, Ch., sess. ord. 1990-1991, n° 1610/1, p. 10).

(43) CNIL, *12ème rapport d'activités-1991*, Paris, Doc. Fr., 1992, p. 112.

35. Toutefois, au vu des difficultés particulières reprises ci-dessus, il semble que certaines garanties particulières devraient accompagner la mise en oeuvre de tels traitements:

1) Le client devrait être informé que des données qui le concernent vont être utilisées aux fins de prospection commerciale(44). Cette information aura lieu sur base de l'article 4, 3° de la loi si la banque s'apprête à utiliser à ces fins les données collectées directement auprès du client. Si la banque omet de l'informer de cette finalité lors de la collecte ou si elle n'avait pas l'intention de la poursuivre à ce moment, elle sera, le cas échéant, tenue de le faire sur base de l'article 9 de la loi.

Ce dernier article impose l'information de la personne lorsque des données qui la concernent sont enregistrées pour la première fois dans un traitement déterminé. Cette condition pourrait viser deux cas de figure. La finalité distinguant les traitements entre eux, il faut en conclure qu'il y aura une nouvelle information lorsque des données seront utilisées pour une finalité distincte de celle poursuivie à l'origine. Cette information devra également avoir lieu en cas d'enregistrement des données dans un traitement qui poursuit certes la même finalité mais est mis en oeuvre par un maître du fichier différent. Il s'agit alors également d'un traitement distinct.

Toutefois, l'article 9, 2° prévoit une exemption à cette obligation d'information lorsque "le traitement se situe dans une relation contractuelle entre la personne concernée et le maître du fichier". Le ministre a précisé que la relation contractuelle devait être entendue au sens large(45). Il s'ensuit, d'après lui, que l'obligation d'information reçoit exception chaque fois que l'individu peut raisonnablement s'attendre à ce que le lien entretenu avec le maître du fichier implique l'enregistrement de nouvelles données. Si on applique cette interprétation à notre problématique, une banque pourrait soutenir que la prospection auprès de sa clientèle est couverte par cette exception. En effet, entretenant une relation contractuelle avec sa banque, le client devrait raisonnablement s'attendre à que son organisme le démarche pour d'autres produits.

(44) Article 4.2 de la Recommandation n° R (85) 20 (marketing direct); article 4.2 de la Recommandation n° R (90) 19 (moyens de payement).

(45) *Doc. Parl.*, Sén., sess. extr., 1991-92, n° 445-2, p. 93.

Cette interprétation nous paraît erronée pour deux raisons. Premièrement parce qu'elle se base sur une lecture trop extensive au vu du libellé du texte qui parle exclusivement de relation contractuelle dans laquelle s'inscrit le traitement. Soit le contrat existe de par l'accord de deux volontés sur un objet déterminé, soit il n'existe pas. Le marketing direct est en marge de la relation contractuelle qui lie le client à sa banque. Le démarchage auprès d'un client tend à une nouvelle relation contractuelle mais n'apparaît pas comme une émanation de la première. Il est vrai que le démarchage est facilité par cette relation mais il ne participe pas à cette dernière. Il en serait autrement si la banque obtenait auprès d'un tiers des données utiles à la gestion de cette relation. On pense par exemple à une banque en phase contentieuse qui obtient d'une autorité publique la nouvelle adresse de son client, adversaire à la cause(46). L'enregistrement de cette donnée pour la première fois, n'implique évidemment pas une information spécifique. Deuxièmement, cette interprétation conduit à nier la ratio de l'article 9. Le but est ici de permettre à la personne concernée de savoir ce que l'on fait de ses données en vue d'en contrôler l'usage. Il ne peut être atteint si l'individu n'est pas au courant de toutes les finalités poursuivies par le maître du fichier(47).

Notons encore que l'information du client s'effectuera indirectement par l'intermédiaire du numéro d'identification du traitement automatisé présent sur toute pièce qui en matérialise l'usage(48). Par ce biais, le client pourra s'informer facilement auprès du registre tenu par la Commission de protection de la vie privée. Cette seule information serait toutefois partielle et n'est pas adaptée à toutes les techniques de marketing direct. Elle suppose que le client soit mis en présence d'une pièce matérialisant le traitement. Cela sera parfois impossible notamment en cas de démarchage téléphonique.

(46) Nous ne tenons pas compte ici des problèmes de légitimité propres aux transferts de données du secteur public au secteur privé.

(47) Une autre question est de savoir si l'exception concernant la relation contractuelle est fondée ou pas. Nous laissons le lecteur libre de son opinion. Le texte étant ce qu'il est, la seule interprétation possible nous paraît être celle qui vient d'être énoncée.

(48) Article 18 al. 4 de la loi.

L'information de la Commission de protection de la vie privée est par contre assurée par l'obligation de déclaration qui pèse sur le maître du fichier(49).

2) Il serait nécessaire de reconnaître, à tout moment, un droit d'opposition à la personne concernée par les données. Ainsi, le client de la banque pourra choisir de ne pas faire l'objet de démarchages commerciaux ou revenir sur son consentement. Le droit d'opposition n'est pas repris dans la loi du 8 décembre 1992. Le ministre responsable du projet le justifie eu égard au caractère "répressif" de la loi; tout traitement est permis *a priori*. Cependant, il n'a pas écarté l'idée que le droit d'opposition soit prévu dans un code de conduite(50).

L'expérience étrangère montre que le droit d'opposition offre une réponse valable aux problèmes spécifiques engendrés par le marketing direct. La C.N.I.L. tente depuis longtemps de généraliser ce droit par la constitution de systèmes "stop publicité"(51). On remarque la même évolution dans les autres pays européens(52). Le droit d'opposition est également prévu à l'article 4 de la Recommandation n° R (85) 20 du Conseil de l'Europe relative au marketing direct et à l'article 4.2 de la Recommandation n° R (90) 19 relative aux opérations de payement.

Par ce biais, la personne concernée par les données reprend en quelque sorte la maîtrise de son image informationnelle. Certains pourraient y voir la négation de l'intérêt économique en jeu entraînant une rupture d'équilibre au profit de l'individu. Tel n'est pas notre sentiment. Le marketing direct s'effectue dans le seul profit - ou espoir de profit - de la banque qui le met en oeuvre. Contrairement aux autres finalités distinguées précédemment, le client n'en retire aucun avantage. Il s'ensuit que l'équilibre des intérêts en jeu va se rompre d'autant rapidement que

(49) Article 17 de la loi.

(50) *Doc. Parl.*, Sén., sess. extr., 1991-92, n° 445-2, p. 50.

(51) Mis en oeuvre dès 1978, son efficacité n'est pas encore totale. Voir par exemple CNIL, *12ème rapport d'activités-1991*, Paris, Doc. Fr., 1992, p. 143 et svtes; voir aussi *10ème rapport d'activités-1989*, Paris, Doc. Fr., 1990, p. 10.

(52) CNIL, *12ème rapport d'activités-1991*, Paris, Doc. Fr., 1992, p. 112; voir aussi l'article 15.3 de la Proposition modifiée de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (COM (92) 122 final - SYN 287, *J.O.C.E.*, n° C 311 du 27.11.1992, p. 30 et svtes).

la vie privée de l'individu est peu ou prou énervée. L'appréciation de cette atteinte est éminemment subjective et dépendra presqu'entièrement du cas d'espèce. La plupart des individus s'accommodent bien du marketing direct. D'autres ne le supportent pas. Dans ce contexte, attendre l'incident pour régler le problème *a posteriori* poserait des difficultés pratiques insurmontables. Dès lors, la solution la plus efficace est de laisser l'individu seul maître de la légitimité du démarchage à son égard.

3) La banque ne devrait utiliser son fichier "clientèle" à des fins de marketing direct que pour promouvoir des produits ou services propres à ses activités(53). Il semble en effet que dans le cas contraire, il y ait déséquilibre entre l'intérêt économique du banquier et l'intérêt individuel de la clientèle. Le tribunal de grande instance de Rennes a parfaitement explicité cette idée dans une affaire où le gérant d'une Caisse d'épargne avait utilisé son fichier clientèle afin de promotionner des ionisateurs d'atmosphère. L'attendu suivant est significatif "Attendu que l'envoi de publicités étrangères aux activités propres d'un établissement à un nombre important de clients répertoriés dans un fichier informatique et n'y figurant que parce qu'ils ont contracté avec cet établissement dans un but précis, les opérations bancaires en l'espèce, est de nature à porter atteinte aux droits des consommateurs; que ceux-ci n'ont pas à être importunés jusque dans le courrier relatif à ces opérations bancaires par des publicités dont l'une était de surcroît en l'espèce d'un goût douteux"(54).

(53) Voir l'article 4.2 de la Recommandation n° R (90) 19 (moyens de payement); voir aussi l'article 2. c de la norme française simplifiée n° 13 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit (*J.O.*, brochure Informatique et Libertés n° 1473, éd. Juillet 1991, p. 169).

(54) T.G.I. Rennes, 8 décembre 1988, *in* CNIL, *9ème rapport d'activités-1988*, Paris, Doc. Fr., 1989, p. 402 et 403; la C.N.I.L. avait déjà déclaré qu'une banque ne peut utiliser son fichier de titulaires de cartes bancaires dans le cadre d'opérations de publipostage pour le compte de commerçants ni, pour le compte d'une société immobilière, effectuer des actions de prospection auprès des titulaires de plan-épargne logement (CNIL, *8ème rapport d'activités-1987*, Paris, Doc. Fr., 1988, p. 170).

La détermination des traitements

36. Comme il a été dit plus haut, la détermination des traitements automatisés utilisés aux fins de marketing direct n'est pas chose aisée. Une distinction semble devoir être faite entre les traitements mis sur pied en vue de prospecter les clients de la banque et ceux qui ne le sont pas. Seuls les premiers retiendront notre attention.

Remarquons tout de même que la prospection auprès de non-clients pose des problèmes particuliers en ce qui concerne le rassemblement des informations. Dans cette hypothèse, les banques devront s'approvisionner exclusivement auprès de fichiers détenus par des tiers. On rentre alors dans la problématique des communications de données à caractère personnel entre différents maîtres du fichier. La difficulté s'accroît encore lorsque la source des données se situe dans le secteur public(55).

37. Peut-on alors accepter qu'une banque ne mette en oeuvre que deux traitements marketing distincts l'un à finalité "prospects", l'autre à finalité "marketing direct auprès de la clientèle"?

Il convient une fois de plus de revenir aux principes directeurs de la détermination des finalités. Le principe de transparence veut que le client ainsi que les organes de contrôle aient une vision suffisamment précise du but d'utilisation pour exercer leurs droits ou leurs missions. Le principe de conformité exige que seules soient traitées les données adéquates, pertinentes et non excessives par rapport au but d'utilisation. Ces exigences sont confrontées ici à une réalité particulière. S'il est possible de prévoir à l'avance les types de données issus du fichier clientèle utilisables à des fins de marketing, il est impossible de

(55) Voir sur ce point la Recommandation n° R (91) 10 du Conseil de l'Europe sur la communication à des tierces personnes de données à caractère personnel détenues par les organismes publics adoptée par le Conseil des ministres le 9 septembre 1991; en doctrine, voir aussi Y. POULLET, "Commercialisation des données détenues par le secteur public - Légitimités et conditions", in *Le Droit de la Concurrence et les Services d'Information*, Actes de la XVIème Réunion annuelle de l'Institut - Paris, les 27 et 28 octobre 1992, en cours de publication; Th. DAVIO, C. DE TERWANGNE, Y. POULLET, "Pour un cadre juridique d'une politique de diffusion des données détenues par le secteur public", *Cahiers Lamy du droit de l'informatique*, n° I, décembre 1991, p. 1 à 8; J. HUET et H. MAISL, *Droit de l'informatique et des télécommunications*, Paris, Litec, 1989, p. 577 et svtes.

déterminer *a priori* les produits spécifiques dont la promotion nécessitera l'utilisation de ces données. Or, la nature du produit déterminera largement la correcte application du principe de conformité. Un produit crédit tend à légitimer l'utilisation d'informations relatives à la solvabilité du client. Il n'en est pas de même d'un produit *sans risques* comme un compte-jeune. De plus, le démarchage est ponctuel. Il n'implique pas nécessairement que les fichiers marketing utilisés soient conservés suffisamment longtemps pour que le client puisse exercer ses droits. Ces finalités instables et évolutives demandent sans aucun doute une adaptation des principes de la loi du 8 décembre 1992.

38. Sans prétendre apporter dès maintenant une réponse à cette difficulté, il nous paraît intéressant de dégager certaines pistes relativement à notre hypothèse de travail.

Certaines données à caractère personnel dont dispose la banque paraissent excessives par rapport aux finalités "marketing direct". Nous pensons particulièrement à celles qui se dégagent de l'utilisation des moyens de paiement. Toutefois, une distinction semble s'imposer entre les informations contenues dans les ordres et celles, objectives et techniques, qui découlent de la manière dont le client utilise les moyens de payement. Une image permettra de faire comprendre la portée de cette distinction. Lorsqu'un client donne un ordre de virement, la situation est analogue à l'envoi d'une carte postale. La banque exécute le virement comme la poste achemine la carte vers son destinataire. Seules les informations nécessaires au service doivent être utilisées par le prestataire. Comme nous le verrons plus en détail dans la seconde partie, les données servant à l'identification des parties peuvent, après traitement, faire apparaître des informations aussi diverses que les habitudes de consommation, les services obtenus auprès de la concurrence ainsi que leur prix, etc. Il suffirait par exemple de relever le montant des primes d'assurances payées par l'individu pour lui faire une offre plus avantageuse...Ces informations secondaires ne sont pas, en tant que telles, destinées aux banques. Toutefois, comme le texte de la carte postale est accessible à la poste, ces informations deviennent "lisibles" pour les banques sans trop de problèmes.

A notre avis, le traitement de ces données pour des finalités marketing déséquilibre les intérêts en présence. Par contre, les

informations qui se dégagent de l'utilisation des moyens de paiement et qui se comprennent comme des données purement techniques, pourraient être traitées. On pense ici par exemple aux types de moyens de paiement utilisés par la personne et à l'analyse des préférences du client par le biais d'une étude de la manière dont ils les utilisent(56).

39. En attendant une prise de décision ferme des autorités de contrôle concernant le nombre de traitements marketing à déclarer, une solution simple pourrait découler du modèle présenté ici. Il est certain que l'analyse de la légitimité des finalités et surtout de la conformité des données utilisées varie en fonction des produits promotionnés. Dans ce contexte, il suffirait de déclarer une finalité marketing et prospect pour chaque type de produit (à risques, sans risques et aide à la gestion du patrimoine). La conformité des données utilisées aux fins de marketing serait alors calquée sur celle de la gestion du produit lui-même. Si la banque promotionne un nouveau crédit, il semble nécessaire et non excessif de se pencher sur les informations relatives à la solvabilité de ses clients avant de les démarcher. Ce ne serait pas le cas pour la promotion d'un nouveau compte épargne.

40. Il est difficile d'aller plus loin dans l'analyse des problèmes liés au marketing direct. Un régime particulier devra être pensé par les autorités de contrôle en collaboration avec le secteur du marketing direct mais aussi, de manière générale, avec des représentants de tous le secteurs d'activités (privé et public) qui utilise d'une manière ou d'une autre les techniques du marketing direct.

c) Les communications aux tiers

41. La communication de données à des tiers pose de nombreux problèmes particuliers au vu de la loi du 8 décembre 1992. Un flou

(56) Dans le même sens, voir CNIL, *12ème rapport d'activités-1991*, Paris, Doc. Fr., 1992, p. 112; *contra* la Recommandation n° R (90) 19 (moyens de payement) qui permet l'utilisation à des fins de marketing direct des informations générées par l'utilisation des moyens de payement sauf en ce qui concerne les données sensibles énumérées à l'article 6 de Convention n° 108 du Conseil de l'Europe (jeu des articles 4.3 et 4.4).

artistique règne tant sur la portée des termes utilisés que sur le régime qui lui est applicable(57). L'étude complète de cette problématique sortirait largement du cadre limité de cette analyse.

La communication rend particulièrement périlleux le contrôle des données par la personne concernée comme par les autorités de contrôle. Elle implique une dilution des données entre maîtres du fichier différents qui peuvent avoir des conséquences néfastes pour l'individu. Aussi, des règles spécifiques sont prises pour en assurer la transparence. De plus, la question de la légitimité de ces transmissions se pose souvent avec beaucoup d'acuité. Pensons à une possible transmission de données relative à la clientèle d'une banque à des entreprises de vente à distance ou à une société de recouvrement.

43. On peut distinguer deux types de communication particulières. Dans un premier cas, la communication constitue véritablement la finalité du traitement. Ainsi, des données à caractère personnel relatives à la solvabilité de la clientèle d'une banque se verront rassemblées et classées afin d'être transmises à d'autres banques en vue de couvrir le secteur contre les risques liés à l'octroi de crédit. Cette transmission constitue une communication particulière en ce sens qu'elle est effectuée dans un but différent de la gestion du produit proprement dite. Le but de la communication est ici recherché pour lui-même et représente la finalité de ce genre de traitement.

Dans un second cas, la communication des données est nécessaire à l'accomplissement d'une finalité distincte. Une banque, en vue d'effectuer un payement international, transmet différentes données à une consoeur étrangère pour les besoins de l'opération. La finalité du traitement est ici de gérer le service proposé à la clientèle, à savoir le suivi de leurs opérations de compte.

(57) Pour une tentative de solution voir M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, "La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel", *J.T.*, 1993, à paraître; De manière plus générale, voir Th. LEONARD et Y. POULLET, *op. cit.*, p. 264 et svtes.

43. Seule la première hypothèse retiendra ici notre attention. Ces transmissions de données à caractère personnel représentent des traitements spécifiques dont les finalités se distinguent de celles analysées jusqu'ici. Tant le principe de transparence que le principe de finalité demandent que ces traitements soient appréhendés de manière spécifique. On peut déterminer deux catégories de communication génératrices de traitements de données à caractère personnel. Les premières sont faites au nom d'un intérêt collectif, les autres au nom de l'intérêt particulier du maître du fichier qui a l'initiative de la transmission.

44. Les communications faites au nom d'un intérêt collectif ou général trouveront généralement une base légale comme fondement de leur légitimité. On pense aux traitements de données à caractère personnel effectuées en vue de l'archivage imposé par la loi fiscale. Dans un autre registre, la loi du 12 juin 1991 relative au crédit à la consommation exige que la banque agissant en tant que prêteur de produits régis communique certaines données relatives aux défauts de payement de sa clientèle à la Banque nationale de Belgique(58). Ce système permet d'une part d'éviter que le consommateur en question ne sombre plus avant dans la spirale du surendettement et d'autre part que le prêteur lui-même n'accorde ses prêts sans espoir de remboursement. La loi du 12 juin réglemente précisément cette communication; elle constitue un traitement particulier. Parfois aussi, le secteur bancaire prend lui-même l'initiative de centraliser des données à caractère personnel en les rendant accessibles à un nombre variable de destinataires. On pense en Belgique au fichier des incidents de paiement tenu par l'Union Professionnelle du Crédit(59). On constate aussi en France l'émergence de fichiers de

(58) Article 71 §1 de la loi du 12 juin 1991 ; voir plus généralement sur cette législation P. DEJEMEPPE, "La mémoire de l'argent - La protection des données à caractère personnel dans la loi du 12 juin 1991 relative au crédit à la consommation", *D.C.C.R.*, Janvier 1992, n° 14, p. 890 à 909; "Crédit à la consommation : de nouvelles données", *D.C.C.R.*, Janvier 1993, p. 102 à 113; E. MEYSMANS, "De verwerking van persoonsgegevens inzake consument krediet", *Computerrecht*, 1993/1, p. 2 à 7.

(59) Notons que l'U.P.C. tombe, en ce qui concerne les produits régis, sous le champ d'application du Chapitre VI de la loi du 12 juin 1991.

cartes ou de chèques volés(60). Toutes ces communications particulières se traduisent au vu de la législation générale comme des traitements de données à caractère personnel ayant pour finalité le but de la communication.

45. Certaines communications viseront uniquement à poursuivre un intérêt particulier de l'organisme financier. C'est le cas des communications de données entre la banque et une compagnie d'assurance, une agence de voyage ou un tiers quelconque. Ce sont ces transmissions qui poseront le plus de problèmes au vu des principes de légitimité et de conformité. Une analyse au cas par cas s'impose alors. Le banquier devra démontrer un intérêt au moins équivalent aux intérêts individuels en jeu s'il veut éviter la censure des autorités de contrôle. Quoiqu'il en soit, ces communications, indépendantes des finalités originelles pour lesquelles les données on été rassemblées, doivent être également perçues comme constitutives de traitements au sens de la loi(61).

Section 3. Vers une remise en question de la vision globale de la clientèle ?

46. Nous avons d'abord analysé la manière dont les banques géraient les données relatives à leur clientèle. Nous avons ensuite tenté de déterminer les catégories de traitements qu'elles mettent en oeuvre pour y parvenir. On constate *a priori* un paradoxe : à l'unité de l'outil et à la vision globale de la clientèle répond une multitude de traitements automatisés au sens de la loi. Chaque traitement automatisé implique une approche différente en ce qui concerne la quantité et la qualité des données pouvant être utilisées, les personnes autorisées à y accéder, la durée de conservation des données, etc. Comment doit-on alors comprendre la vision globale des données relatives à la clientèle ?

(60) Voir par exemple, CNIL, *8ème rapport d'activités-1987*, Paris, Doc. Fr., 1988, p. 163 et svtes; CNIL, *10ème rapport d'activités-1989*, Paris, Doc. Fr., 1990, p. 129 et svtes; *12ème rapport d'activités-1991*, Paris, Doc. Fr., 1992, p. 96 et svtes.

(61) Pour un cas récent dans la jurisprudence française où le juge vient censurer la communication de données relatives à la clientèle d'une banque à des commerçants, voir Rennes, 13 janvier 1992, *Expertises*, fév. 1993, p. 76 à 78 et note J. FRAYSSINET.

47. La réponse doit être nuancée. L'étude des implications de la loi du 8 décembre 1992 dans le secteur bancaire débute à peine. De nombreuses inconnues vont subsister dont la moindre n'est pas l'interprétation de la loi par les autorités de contrôle. Dès lors, il est prémonitoire d'avancer des conclusions trop hâtives. Les banques doivent cependant s'organiser dès aujourd'hui pour appliquer la loi. Une interprétation des principes directeurs de la loi nous pousse à répondre que la vision globale des données relatives à un client doit rester possible (1) mais être encadrée (2) et sans doute limitée (3).

1) La gestion des produits bancaires se fonde sur la confiance réciproque des acteurs (banquier et client). Cette confiance peut être ébranlée pour de multiples raisons. Elles seront le plus souvent objectives (situation d'insolvabilité manifeste se concrétisant par des comptes non approvisionnés, des échéances de remboursement non respectées, etc.) mais aussi parfois subjectives (sentiment de méfiance fondé sur des impressions propres au banquier). L'outil informatique permet de fixer et de visualiser aisément les traces des événements susceptibles de remettre cette confiance en question. Les raisons objectives se fonderont sur les informations rassemblées auprès du client ou de tiers au fur et à mesure de la relation puis traitées pour les finalités susmentionnées. Les raisons subjectives elles-mêmes - qui restaient volatiles sans l'aide de l'informatique - peuvent maintenant être enregistrées quelque part dans la mémoire de l'ordinateur.

La vision globale de la clientèle n'est en fait rien d'autre qu'un traitement automatisé de données à caractère personnel ayant pour finalité générique la mesure de la confiance que la banque peut mettre en sa clientèle. Plus précisément, ce traitement peut s'analyser en un système d'aide à la décision encore rudimentaire. Il permet d'accéder à un ensemble de données à caractère personnel facilitant ainsi la prise de décisions par le banquier (puis-je accorder au client un nouveau crédit, dois-je prendre des mesures d'exécution à son encontre, sa situation peut-elle s'améliorer, puis-je encore le solliciter pour d'autres produits, etc.). Le système de la vision globale ne donne pas comme telle une réponse aux interrogations du banquier. Il lui permet par contre d'asseoir une décision qu'il reste seul à prendre sur base d'un maximum d'informations. Dès lors, se poser la question de savoir si la vision globale doit être

permise revient à s'interroger sur la légitimité de la finalité poursuivie par un tel traitement.

Le banquier commet-il une ingérence excessive dans la vie privée de son client en s'aidant de l'outil informatique pour orienter la confiance à mettre en lui? On retrouve en filigrane la problématique des profils servant de fondement à la prise d'une décision.

La proposition de Directive européenne consacre son article 16 à cette difficulté. Cette disposition demande notamment aux Etats membres de conférer à la personne concernée par les données le droit de ne pas être soumise à une décision privée lui faisant grief si deux conditions sont remplies: la prise de décision s'effectue sur le seul fondement d'un traitement automatisé; ce dernier définit un profil de personnalité. Toutefois ce principe peut recevoir exception dans deux cas de figure. Le premier vise l'hypothèse où la décision est prise dans le cadre d'une relation contractuelle. Il faut toutefois que la demande de la personne ait été satisfaite ou, dans le cas contraire, "que des mesures appropriées, parmi lesquelles la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime".

La loi française, en son article 2 alinéa 2, prévoyait déjà le même principe quoiqu'en des termes un peu différents(62). Aucune exception n'est toutefois prévue. Il faut également se rappeler que la loi française permet à la personne concernée de contester le raisonnement utilisé dans le traitement automatisé dont les résultats lui sont opposés(63).

Ces deux textes ont le même fondement: s'assurer que l'être humain conserve la pleine maîtrise de décisions qui s'imposent à d'autres(64). La légitimité des systèmes experts et autres systèmes d'aide à la décision trouve là à la fois sa condition et sa limite. Tant que

(62) "Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé".

(63) Article 3.

(64) Voir en ce sens CNIL, *Dix ans d'informatique et libertés*, Paris, Economica, 1988, p. 46; Proposition modifiée de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Exposé des motifs, *inédit*, p. 26.

l'outil ne prend pas la place du décideur, l'utilisation de l'outil informatique doit être permise sous peine de nier l'avance technologique dans ce qu'elle a de meilleur : sa capacité de servir l'être humain dans l'exécution de ses tâches.

La loi belge est muette face à ces difficultés. Toutefois, ces règles pourraient se retrouver *mutatis mutandis* comme conditions de légitimité de tels traitements.

La vision globale des informations concernant un client déterminé ne conduit pas à une automatisation de la décision au sens des législations susmentionnées. Le système informatisé bancaire permet au décideur de se promener au gré des "tiroirs" et d'ainsi accéder à un nombre important d'informations concernant une personne déterminée. Ces procédures automatisés ne jouent alors "qu'un rôle de révélateur dans une décision prise par les instances compétentes après examen approfondi et une instruction contradictoire"(65). La vision globale doit donc, selon nous, être considérée comme légitime.

2) Elle doit être *limitée* car, d'après nous, certaines données ne peuvent pas servir au banquier ou seulement à des fins très précises. Si l'on admet que la vision globale de la clientèle est constitutive en soi d'un traitement automatisé de données, on retrouve ici les exigences du principe de conformité. Les informations qui apparaissent lors de l'utilisation des moyens de payement ou les données nécessaires à un système d'aide au calcul de l'impôt ne pourraient par exemple se retrouver dans la vision globale du client. Ces données apparaissent comme excessives eu égard à la finalité poursuivie; l'intérêt de la personne concernée s'oppose selon nous à ce que le banquier épluche toutes ces informations sous prétexte qu'il a une décision à prendre vis-à-vis de son client.

Parmi la masse de données stockées dans la mémoire du système, il faut déterminer celles qui sont propres à influencer la confiance du banquier envers son client. Il faudra ensuite leur imposer le test de proportionnalité ce qui aura pour conséquences à notre sens d'exclure l'utilisation de types de données telles que relevées plus ci-avant.

(65) CNIL, *Dix ans d'informatique et libertés*, *op. cit.*, p. 48 ; voir les hypothèses citées où la C.N.I.L. a admis que les systèmes mis en place ne contrevenaient pas à l'article 2 de la loi française.

3) La vision globale doit enfin être encadrée. La finalité du traitement qu'elle engendre étant en dernier ressort la prise de décisions concernant la clientèle, seules les personnes compétentes doivent avoir les clés d'accès permettant la constitution de cette vision globale. Les banques devraient donc dans un premier temps déterminer avec le plus grand soin l'organigramme de leur entreprise pour, dans un second temps, accorder un nombre de clés plus ou moins grand selon le niveau de compétence. Une personne qui n'exerce aucune compétence de décision ne devrait donc pas accéder à une vision globale de la situation du client. Par contre, le directeur d'agence éventuellement compétent pour accorder un prêt devrait pouvoir y accéder. On retrouve là l'obligation légale mise à charge du maître du fichier de "limiter l'accès aux seules personnes, qui en raison de leur fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées"(66).

48. La vision globale envisagée comme un traitement automatisé spécifique se superpose aux différents traitements automatisés identifiés plus avant. Notons qu'elle ne se confond pas avec ces derniers même si elle trouvera parfois à s'appliquer concomitamment à l'un de ceux-ci. Ainsi par exemple, l'octroi et la gestion d'un produit *à risque* s'accompagne d'une prise de décision quant à la solvabilité du client. Les données nécessaires feront dès lors l'objet de deux traitements distincts. L'un a trait à la gestion du produit en ce compris l'analyse de la solvabilité au sens strict (par exemple le recours au crédit-scoring). L'autre a pour but la prise de décision elle-même et permettra l'accès à toute information qui, dans le respect des droits individuels de la clientèle est susceptible d'influencer la confiance à accorder au client en question (résultats du scoring, avoir en compte, etc.).

Nous terminerons cette partie par une dernière interrogation. Pour une banque fonctionnant telle que nous l'avons décrite, on peut se demander s'il n'existe pas une summa divisio relative aux différentes catégories de traitements mis en oeuvre : ceux qui visent à la prise d'une décision concernant la clientèle et ceux qui ne visent qu'un but fonctionnel c'est-à-dire la gestion des produits offerts au sens strict. Chacune des deux catégories appelle la prise de mesures qui lui sont propres. Les véritables

(66) Article 16 §1 4°, voir aussi l'article 17 §2, 7°.

difficultés interviennent alors lorsque les informations nécessaires à l'une sont utilisées pour l'autre.

CHAPITRE II
TRAITEMENTS DE DONNEES SENSIBLES ET UTILISATIONS DES MOYENS DE PAIEMENT

49. La loi prévoit en ses articles 6, 7 et 8 un régime particulier en ce qui concerne certaines catégories de données à caractère personnel. Le législateur s'est fondé sur le fait que "certaines données touchent à ce point à la personnalité intime de l'individu que leur enregistrement, leur traitement ou leur diffusion font objectivement craindre une possibilité de discrimination"(67). Les articles 7 et 8 relatifs aux données judiciaires et médicales ne retiendront pas ici notre attention(68). Nous nous limiterons à l'analyse des problèmes engendrés par l'article 6 lors de la gestion d'opérations de payement.

Section 1. Le régime des données sensibles énumérées à l'article 6

50. L'article 6 énonce que "le traitement de données à caractère personnel relatives aux origines raciales ou ethniques, à la vie sexuelle, aux opinions ou activités politiques, philosophiques ou religieuses, aux appartenances syndicales ou mutualistes n'est autorisé qu'aux fins déterminées par ou en vertu de la loi". La Commission de protection de la vie privée rend un avis préalable chaque fois que les finalités sont déterminées en vertu de la loi. En outre, le Roi pourra prévoir des conditions particulières relatives aux traitements dont la finalité est déterminée par ou en vertu d'une loi. Dans ce cas, il s'exécutera par arrêté délibéré en Conseil des ministres après avis de la Commission de la protection de la vie privée.

(67) Exposé des motifs, *Doc. Parl.*, Ch. Repr., sess. ord. 1990-1991, n° 1610/1, p. 11.

(68) Sur celles-ci voir M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, "La loi du 10 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel", *J.T.*, 1993, à paraître.

51. Contrairement à la philosophie de la loi, le traitement des données sensibles n'est pas libre. La protection ne se fonde plus ici sur un contrôle *a posteriori*. La loi recherche dans l'intervention du législateur une garantie aux risques de discrimination présents en germe dans la nature de certaines données. Ainsi, une loi doit impérativement déterminer les buts d'utilisation légitimes de ces données. Cette compétence peut également être déléguée au Roi. Cette délégation doit être bien comprise. La loi du 8 décembre ne suffit pas à elle seule pour fonder celle-ci(69). Il faudra nécessairement qu'une loi particulière délègue expressément cette compétence. Ainsi, en toute hypothèse, le traitement des données énumérées à l'article 6 trouvera sa source dans une loi.

Section 2. La problématique des opérations de payement

52. Les opérations de payement présentent la particularité de faire apparaître certaines informations dont l'importance et la nature seront variables suivant le moyen de payement utilisé (comptant, chèques, virements, T.E.F.)(70). Mis à part le payement au comptant, ils permettront tous au banquier de connaître le destinataire du payement et donc, le cas échéant, l'objet de la transaction(71). La gestion d'un moyen de payement nécessite de l'information pour être menée à bien dont celle relative à l'identification des parties à la transaction. Elle ne requiert par contre aucune information relative aux opinions politiques, sexuelles, religieuses ou autres des personnes parties à la transaction. Toutefois, de telles informations peuvent apparaître dans l'esprit de celui qui consulte les données utilisées à des fins de gestion du moyen de payement. Ainsi, un payement relativement faible effectué par un individu

(69) Contrairement à ce qui est prévu à l'article 8 §5 concernant les données judiciaires où un Arrêté Royal suffit. Remarquons que le ministre lui-même distingue ces deux hypothèses dans son exposé introductif en Commission de la Justice de la chambre (*Doc. Parl.*, Ch. Repr., sess. extr. 1991-1992, n° 413/12, p. 11). Ainsi, il déclare que "Dans les cas où la loi n'aurait rien prévu, autorisation peut être accordée par le Roi sur avis de la Commission. Cela est prévu pour prévenir l'immobilisation complète, mais concerne *uniquement les données policières et judiciaires*. Pour les données très sensibles visées à l'article 7 (*ndlr* le nouvel article 6), *il n'est pas prévu de dérogation par arrêté royal*".

(70) Y. POULLET, "T.E.F. et protection des données à caractère personnel", *op. cit.*, p. 181.

(71) Le virement papier est plus explicite puisqu'il comprend une communication qui, lorsqu'elle n'est pas chiffrée, révèle souvent l'objet de la transaction.

au profit d'un parti politique, fût ce sans communication, engendrera dans l'esprit de celui qui en a connaissance une nouvelle information : monsieur X a vraisemblablement telle ou telle opinion politique puisqu'il paye sa cotisation au parti. C'est pourquoi l'article 6 est de nature à alarmer plus d'un banquier(72). En effet, certains modes de payement risquent bien de faire apparaître des informations considérées comme sensibles par la loi. Ainsi, si un membre d'un syndicat paye sa cotisation annuelle par virement. De même pour le membre d'une organisation religieuse ou le lecteur d'un journal à tendance.

Notons que lorsque l'opération s'effectue par les biais d'une automatisation complète, l'information sensible passera le plus souvent inaperçue. L'ordinateur n'a pas la capacité de la comprendre ; ces trois données ne représentent rien d'autre pour lui que des éléments codés nécessaires à une application spécifique. Elle est seulement compréhensible pour l'employé qui visualiserait l'ordre de payement, ce qui nécessiterait de sa part diverses manipulations. En cas de virement papier l'information se révèle plus directement : l'employé devra lire les informations afin de vérifier si le compte du donneur d'ordre est suffisamment approvisionné puis ensuite, le cas échéant, pour exécuter l'ordre. Quoiqu'il en soit, dans tous ces cas, la banque a les moyens de prendre connaissance de l'information sensible.

53. La solution de ce problème se perçoit grâce à un cheminement en deux temps. Pour que l'article 6 s'applique il faut nécessairement que l'information soit une donnée et qu'elle fasse l'objet d'un traitement. Si, dans l'hypothèse de départ, la première condition semble remplie, la seconde fait défaut.

(72) Voir par exemple E. MEYSMANS, "De wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens - Gevolgen voor de banksector", in *Journée d'étude du 18 mars 1993*, Association Belge des Banques, à paraître ; déjà dans "Bancaire bestanden en privacy-bescherming in België", *Computerrecht*, 1992, n° 1, p. 11 et 12.

A. Le concept de donnée

54. Une nouvelle information, résultant du rapprochement intellectuel de données qui lui sont *a priori* étrangères est-elle une donnée au sens de l'article 1 § 5 de la loi ? La loi du 8 décembre 1992 ne définit pas le concept de « donnée ». Il reviendra donc à la doctrine ou aux organes de contrôle de l'interpréter.

55. Pour l'informaticien, les concepts de données et d'information doivent être soigneusement distingués. La donnée est "un fait, une notion, une instruction *représentée sous une forme conventionnelle*(73), convenant à une communication, une interprétation ou un traitement soit par l'homme, soit par des moyens informatiques"(74). L'information est quant à elle "tout le signifiant que l'on attache et que l'on peut déduire d'un ensemble de données, de certaines associations entre données"(75). Dans cette conception, la donnée vient formaliser l'information qui, par essence, est immatérielle. La donnée est matérialisée par le support qui la contient ; elle confère une assise matérielle à une ou plusieurs informations(76).

(73) C'est nous qui mettons en italique.

(74) Définition proposée par l'Association Française de Normalisation (AFNOR), citée par J.-M. BUSTA et S.-M. MIRANDA, *L'art des bases de données*, Paris, Eyrolles, vol. 1, 4ème édition, 1990, p. 12 ; les auteurs parlent aussi de "l'enregistrement dans un code convenu d'une observation, d'un objet ou d'un phénomène (donnée « factuelle ») d'une image, d'un son, d'un texte" ; voir aussi F. BODART et Y. PIGNEUR (*Conception assistée des systèmes d'information-Méthode-Modèles-Outils*, Paris, Masson, 2ème éd., p. 13) qui définissent le terme de donnée comme étant la "représentation (codée) des propriétés - y compris l'existence - d'un concept, d'un objet, d'un fait ou d'un événement".

(75) J.-M. BUSTA et S.-M. MIRANDA, *op. cit.*, p. 13 ; voir aussi F. BODART et Y. PIGNEUR, *op. cit.*, p. 14 où l'information est définie comme la "signification potentielle attachée aux données, susceptible d'affecter le comportement des hommes et des machines dans une organisation".

(76) Cela découle également de la définition de la donnée au sens informatique retenue par le Petit Robert (1988) : "la représentation conventionnelle d'une information (fait, notion, ordre d'exécution) sous une forme (analogique ou digitale) permettant d'en faire le traitement automatique".

56. Les législations "vie privée" ne semblent pas retenir cette distinction. Au contraire, pour elles, le concept de donnée s'identifie à celui d'information. Ainsi, d'après la Convention n° 108 du Conseil de l'Europe, la donnée vise "toute information"(77). De nombreuses autres réglementations, nationales ou internationales, procèdent de la même façon(78). En mettant sur pied d'égalité deux concepts représentant au sens technique deux réalités différentes, les lois "vie privée" paraissent *a priori* ambiguës. Donnent-elles la suprématie à l'élément matériel contenu dans le concept technique de donnée ou à l'élément immatériel contenu dans celui d'information?

Les lois "vie privée" se veulent indépendantes de l'avancement technologique. Elle ont un objet plus large que la réglementation de l'outil informatique. Ainsi, elles visent également les traitements non automatisés ou les fichiers manuels. Retenir la notion de donnée informatique comme base du champ de protection n'aurait pas permis ces extensions. Dès lors, ces législations visent directement l'information en elle-même, étant entendu que celle-ci trouvera une assise matérielle via le procédé ou le support utilisé pour son traitement. Elles font ainsi l'économie d'une étape qui ne les intéresse pas: la formalisation ou la codification de l'information.

(77) Article 2. a.

(78) Voir par exemple l'article 2. a de la proposition modifiée de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM (92) 122 final - SYN 287, *J.O.C.E.*, n° C 311 du 27. 11. 1992, p. 30 et svtes; article 3. a de la loi espagnole (Loi organique 5/1992, du 29 octobre, relative au traitement automatisé de données à caractère personnel, *BOE*, n° 262 du 31 octobre 1992, p. 37 037 et svtes); la section 3 (1) de la loi fédérale allemande (Bundesdatenschutzgesetz (Federal Dataprotection Act), 20 décembre 1990, Bundesgesetzblatt, I, 1990, p. 2954 et svtes); les lois françaises et portugaises, quant à elles, n'utilisent même pas le terme de donnée pour lui préférer directement celui d'information (article 4 de la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.*, 7 et rectif. 25 janv. 1978 et article 2. a de la loi portugaise n° 10/91 relative à la protection des informations nominatives face à l'informatique, *J.O.*, I série A, n° 98 du 29 avril 1991); tout comme la loi belge, la loi néerlandaise ne définit pas le concept de donnée (article 1 - Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levensfeer in verband met persoonsregistraties, *Staatsblad*, 1988, 665).

57. On peut dès lors conclure que l'information qui apparaît fugitivement du rapprochement d'autres informations est bien une donnée au sens des lois protectrices de la vie privée. Toutefois, ces législations ne trouveront à s'appliquer que si cette donnée fait l'objet d'un traitement.

B. Le concept de traitement

58. Trois conditions doivent être remplies pour que l'on puisse parler d'un traitement automatisé(79): des opérations (1) doivent être effectuées sur des données à caractère personnel par le biais de procédés automatisés (2) en vue de réaliser une finalité (3). Il a été précisé que la finalité permettait seule de distinguer les traitements automatisés entre eux.

59. Les données "sensibles" qui apparaissent lors des opérations de payement font-elles l'objet d'un traitement spécifique?

Les données qui vont permettre la révélation d'une opinion politique, religieuse, etc. sont, au maximum, au nombre de trois: le nom du donneur d'ordre, celui du bénéficiaire et éventuellement la communication. C'est le rapprochement de ces trois données qui permettra, le cas échéant, l'émergence de l'information sensible. Le traitement ayant pour finalité la gestion du compte ne connaît que les données de bases. Seules celles-ci sont nécessaires à la poursuite de la finalité poursuivie. Il y a donc enregistrement des noms et de la communication, débition du compte du donneur d'ordre, transfert à la banque du destinataire, inscription de l'opération aux fins de création de l'extrait de compte, etc. Aucune de ces opérations ne porte directement sur l'information sensible. Celle-ci est ignorée. Elle existe en germe quelque part dans le système de gestion de l'information mais ne fait l'objet d'aucune opération particulière par le gestionnaire du traitement. On peut donc déjà soutenir que cette information ne fait l'objet d'aucune opération susceptible de faire partie d'un traitement automatisé au sens de la loi.

(79) Cf. supra, n° 10 et svts.

De plus, même à considérer les opérations effectuées sur les données brutes comme portant indirectement sur l'information sensible, force est de constater qu'elles ne seraient transcendées par aucun but d'utilisation. En effet, aucune finalité n'est susceptible d'unifier l'enregistrement, la conservation, voire la consultation de cette donnée. La prise de connaissance de l'information sensible dans le cadre strict de la poursuite de l'opération de payement est purement fortuite. Il en irait tout autrement si le banquier épluchait systématiquement les ordres de payement afin d'en retirer les informations propres à la constitution du profil de ses clients. Dans ce cas, des opérations seraient effectuées sur l'information sensible dans un but prédéterminé. L'ensemble de ces opérations pourrait alors constituer un traitement automatisé à part entière.

60. Ce raisonnement se retrouve en germe dans la Recommandation R (90) 19 du Conseil de l'Europe relative à la protection des données à caractère personnel utilisées à des fins de payement. Deux dispositions particulières ont trait à la problématique des données sensibles.

L'article 3.8 vise la première catégories de données utilisées lors d'une opération de payement : les données qui sont collectées indépendamment de l'utilisation du moyen de payement. Ainsi, les données relatives aux condamnations pénales peuvent être traitées si elles sont de nature à remettre en cause l'opportunité de la fourniture du moyen de payement ou de la poursuite de son utilisation(80). Dans ce contexte, l'alinéa 2 ajoute que la collecte et l'enregistrement des autre données sensibles énumérées à l'article 6 de la Convention n° 108 du Conseil de l'Europe(81) ne devraient pas être permis. La ratio se distingue clairement : ces données ne présentent pas de lien suffisant avec la finalité d'appréciation de la solvabilité du titulaire du moyen de payement(82).

(80) L'article ajoute que dans ce cas, ce traitement ne sera permis que si l'émetteur du moyen de payement obtienne le consentement exprès et éclairé du client ou que le traitement soit conforme aux garanties par le droit interne.

(81) A savoir, les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions et les données à caractère personnel relatives à la santé ou à la vie sexuelle.

(82) Voir Exposé des motifs, n° 50.

L'article 4.4. a trait quant à lui spécifiquement à l'utilisation des données "sensibles" engendrées par l'emploi du moyen de paiement : ces données "ne doivent pas être utilisées à des fins de marketing ou de promotion ou à toute autre fin". Cette disposition pourrait paraître *a priori* en pleine contradiction avec la règle énoncée à l'article 3.8. Pourquoi interdire l'utilisation de données qui ne peuvent ni être collectées, ni être enregistrées ? Selon nous, il n'en est rien. La logique qui sous-tend ces dispositions nous paraît identique au raisonnement développé ci-dessus. Les deux hypothèses sont différentes ; les données visées par l'article 3.8. ne sont pas celles reprises à l'article 4.4. Dans la premier cas, il s'agit de données *a priori* qui feront l'objet du traitement visant à gérer les opérations de payement. Dans le second cas, il s'agit de données qui se révèlent *a posteriori* par l'utilisation des moyens de payement. Il est impossible d'en éviter l'émergence mais elles ne pourront faire l'objet d'une quelconque utilisation par le banquier(83).

Que le problème soit appréhendé via la notion de traitement, comme la loi belge nous y pousse, ou par la nature des données utilisées, le résultat est identique. L'interdiction de traitement ne s'applique que s'il y a réutilisation par le banquier des informations sensibles générées par l'utilisation des moyens de payement. Par rapport au texte de la Recommandation, notre opinion met seulement en avant un élément supplémentaire qui est d'ordre purement conceptuel et théorique : le traitement de l'information sensible n'existe en fait que lors de la réutilisation de l'information qui risque d'apparaître en cours d'utilisation du moyen de payement.

61. Il faut en conclure que le cas de figure décrit ci-avant ne tombe pas sous le champ d'application de l'article 6 de la loi belge. Il n'est donc pas nécessaire qu'une loi vienne légitimer un traitement quelconque de données sensibles par les banques en vue de la gestion des opérations de payement. La personne concernée ne serait d'ailleurs pas mieux protégée dans ce cas. Le véritable problème est celui de la possibilité de récupération ultérieure de l'information qui apparaît lors de l'utilisation des moyens de payement. L'article 6 reprend ici toute son importance. En

(83) Ceci ressort clairement de l'exposé de motifs de la Recommandation (comparez les points 50 et 58).

l'absence d'une loi qui viendrait les légitimer, aucun traitement ne peut porter sur l'information sensible déduite des données de base traitées.

CONCLUSION

62. Le juriste "classique", non initié aux législations "vie privée", sera sans doute effrayé de la marge d'interprétation dont dispose toute personne désireuse de se conformer à la loi du 8 décembre 1992. La fluidité du concept de traitement automatisé comme celle qui entoure la portée du principe de finalité se doivent d'être bien comprises.

L'objet de la législation frappe par son indétermination. La vie "privée" est un concept éminemment relatif qui ne se laisse circonscrire qu'au gré des circonstances particulières. L'analyse des risques d'atteintes à la liberté de la vie privée dépendra largement de la manière dont les données à caractère personnel sont utilisées et des garanties apportées par le maître du fichier quant au respect des principes de protection. De plus, l'homme de loi est bien en peine de définir la réalité technique contre laquelle l'individu est protégé. Cette réalité lui échappe non seulement parce qu'il la connaît mal mais aussi parce qu'il est obligé d'utiliser des concepts suffisamment ouverts pour englober toute la diversité actuelle et future des nouvelles technologies de l'information.

63. On perçoit alors la nature particulière de la loi du 8 décembre 1992. Tout en imposant au maître du fichier de prendre des mesures très précises d'organisation pour s'y conformer, elle n'est porteuse d'aucune règle de conduite certaine concernant les buts d'utilisations des données traitées. La loi détermine un cadre procédural propre à guider, dans le respect des libertés individuelles, les responsables des traitements de données à caractère personnel. La création d'un organe de contrôle *sui generis*, indépendant des détenteurs du pouvoir généré par la maîtrise des techniques informationnelles, trouve ici son fondement. C'est à la Commission de protection de la vie privée qu'il reviendra de déterminer, dans le respect du cadre légal et réglementaire, les limites d'utilisation de l'information. Pour ce faire, elle doit se laisser guider par la recherche d'un équilibre entre les intérêts qui s'opposent.

Le rôle du maître du fichier doit encore être mis en exergue. C'est à lui qu'il revient, avant tout autre, de remettre en question sa gestion des données à caractère personnel. En interprétant la nouvelle législation, il ne peut oublier qu'ici, plus que dans toute autre matière, la philosophie de la protection transcende le prescrit du texte.

64. Bien plus que les ébauches de solutions proposées ici, nous espérons avoir contribué, modestement, à l'émergence d'un modèle théorique propre à guider tout maître du fichier dans sa recherche de détermination des traitements automatisés. Les interprétations proposées peuvent paraître parfois osées; qu'importe si le débat est lancé. La loi du 8 décembre 1992 contient en germe un droit en devenir. Il est temps maintenant de le saisir.