

vege de cliënten van  
aan de toepassing en  
dient gebracht onder  
ook anderszins geen  
lz. 4 nr. 5 en vnml.

ei andere inbreuk op  
f de praktijk door de  
n vinden, zonder tot  
n veranderende han-  
van de aanvaarding  
en de economische  
ervaging, waarop tot  
ide, bovenvermelde  
k op de Privacywet,  
niet i.v.m. marketing

bruik van op onrecht-  
werd weerhouden;

wd het gebruik door  
matie (m.b.t. de ver-  
el) verkregen in het  
iet akkoord van deze  
nden op louter finan-  
e verzekeringssector  
eroepsbelangen van  
enredig groot markt-  
aan de beroepsbelan-  
k het belang van de  
ing (zie de relevante  
ten dage sprake van  
en in de persoonlijke  
alsook van toenemen-  
merkt dat er nog geen  
ding, waar bedoelde  
t;

orgvuldigheidnorm;

ling door verweerster  
lijkende reclame, niet

(...)

Verklaren de eis ontvankelijk en gegrond in volgende mate;

Zeggen voor recht dat het gebruik maken van persoonsgegevens die op betaalopdrachten werden vermeld en die verweerster van haar klanten betreft, met het oog op het voeren van publiciteit en klantenwerving voor het afsluiten en centraliseren van hun verzekeringspolissen bij of via verweerster, een met de eerlijke handelsgebruiken strijdige daad is volgens art. 93 W.H.P.;

Leggen verweerster verbod op nog langer haar klanten bij middel van mailings, publiciteit of op welke wijze ook te benaderen, voor het afsluiten van verzekeringspolissen bij haarzelf of via haarzelf, met gebruikmaking van de op de overschrijvingsformulieren voorkomende gegevens, en dit op straffe van een dwangsom ad 10.000 fr per vastgestelde inbreuk vanaf de betekening van het vonnis;

Veroordelen verweerster tot publicatie op haar kosten van het beschikkend gedeelte van het vonnis in drie dagbladen en dit binnen de acht dagen na betekening van het vonnis, bij gebreke waaraan eiseres wordt gemachtigd de publicatie te doen verrichten op kosten van verweerster;

(...)

7 juli 1994

Zet. : Thibaut

Pleit. : Joris, Huybrechts

Tegen deze beslissing werd beroep aangetekend.

### **Note : La banque, le courtier et la vie privée : une première décision jurisprudentielle**

1. Alors même que l'intégralité de la loi du 8 décembre 1992 n'est pas encore entrée en vigueur, les juridictions judiciaires ont déjà été, par trois fois, amenées à s'interroger sérieusement sur la correcte application de son prescrit(1).

Que les trois premières applications jurisprudentielles de la loi concernent le monde bancaire -au sens large- ne constitue pas une surprise. La nature même des activités poursuivies, impliquant un transfert important d'informations de la clientèle vers l'organisme financier, liée à une utilisation optimale des nouvelles technologies de l'information, jettent ce secteur en première ligne de la phase d'implémentation de la législation protectrice(2).

Que la correcte application de la loi devienne un élément d'appréciation du contrôle des usages honnêtes en matière commerciale pourrait sembler plus étonnant. Le but premier de la loi consiste à protéger l'individu. Dans un marché de l'information en pleine révolution, la donnée à caractère personnel a vu, dans certains secteurs, sa valeur économique croître de manière exponentielle en fonction des nouvelles possibilités d'utilisation induites des

progrès technologiques. La violation des obligations mises à charge des maîtres du fichier, peuvent donner à ceux qui la commettent un avantage certain dans la recherche et l'utilisation des informations personnelles et cela, au détriment des entreprises concurrentes. L'affaire qui donne lieu à ce bref commentaire est significative à cet égard, puisque la loi de protection individuelle se transforme en une arme utilisée par les courtiers d'assurances pour s'opposer à certaines pratiques dérivées de la bancassurance.

2. Les faits qui sous-tendent la décision du Président du tribunal de commerce d'Anvers sont assez simples même s'ils ne ressortent pas clairement du jugement. Une agence locale de la Kredietbank, agissant en tant que courtier d'assurance pour une entreprise tierce, a traité des données relatives à sa clientèle de produits financiers afin de cibler au mieux les personnes susceptibles d'être intéressées par les produits d'assurances proposés. Ces données étaient issues des virements bancaires utilisés pour le paiement de primes d'assurance à des entreprises tierces. Uniprabel, l'association professionnelle des courtiers d'assurance, a vu dans cette pratique un acte contraire aux usages honnêtes en matière commerciale et a, dès lors, intenté une action en cessation devant la juridiction présidentielle. Cette dernière a fait droit à cette demande en se fondant sur la violation de la loi du 8 décembre 1992 et du principe général de prudence qui prévaut en matière de pratiques du commerce. Seul le premier point fera l'objet de nos commentaires.

Le jugement, exécuté par provision, est frappé d'appel. Cette circonstance, liée au tapage médiatique entourant cette affaire, nous pousse à rester prudent dans notre commentaire. C'est d'autant plus nécessaire que l'application de la législation du 8 décembre 1992 aux services d'assurance par les institutions bancaires est bien plus complexe qu'il n'y paraît. Une analyse de fond dépassant de loin celle possible dans une note d'observations s'imposerait idéalement. Toutefois, il n'est pas inutile de relever brièvement les principales options théoriques prises, *in casu*, par le juge, tant au niveau de l'interprétation de la loi que de ses implications en matière de pratiques du commerce.

3. Le jugement commenté met remarquablement en exergue le principe de finalité des traitements énoncé à l'article 5 de la loi.

Cette disposition dispose que "les données à caractère personnel ne peuvent faire l'objet d'un traitement que pour des finalités déterminées et légitimes et ne peuvent être utilisées de manière incompatible avec ces finalités; elles doivent être adéquates, pertinentes et non excessives par rapport à ces finalités". Elle contient deux principes distincts : celui dit de légitimité de la finalité et celui dit de conformité des données(3).

Pour contrôler la correcte application de cette disposition, le juge se doit de rechercher l'exacte finalité énoncée du traitement en cause. De l'analyse de l'état des traitements poursuivis par la banque(4), il appert que seule une

finalité explicitement prévue est susceptible de couvrir le traitement contesté. Celle-ci s'énonce comme suit: "la prospection et la promotion des produits financiers (marketing)".

**1. Le contrôle de légitimité de la finalité : la finalité doit être déterminée**

4. Le principe de légitimité obéit lui-même à deux règles distinctes. La première, formelle, exige que le but poursuivi par le traitement soit clairement déterminé(5). Il s'agit d'une obligation de transparence capitale dans le dispositif 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 de protection de la vie privée ou les juridictions saisies d'un litige.

Cette exigence abstraite se traduit par des obligations concrètes mises à charge du maître du fichier. Ainsi, par exemple, l'état des traitements doit comprendre l'énoncé exact de la finalité. L'obligation d'information de la personne concernée lors de la collecte, insérée par l'article 4 de la loi et rappelée expressément par le juge, implique aussi la communication de la finalité pour laquelle les données sont recueillies.

Deux conséquences en résultent(6). 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. En effet, le principe de finalité implique que les données ne puissent être utilisées de manière incompatible avec la finalité déterminée.

Faisant application de ces règles, le juge constate une double violation de la loi du 8 décembre 1992. Le but d'utilisation réelle des données en cause n'est pas la promotion et la prospection des produits financiers de la banque agissant comme telle (moyens de paiement, prêts, plans d'épargne etc.) mais le marketing de produits d'assurance. Cette finalité réelle est différente de celle énoncée. N'apparaissant nulle part dans l'état tenu par la banque, le juge conclut à une utilisation incompatible des données avec la finalité énoncée. Dans le jargon propre à cette matière, il s'agit "d'un détournement de finalité". L'article 5 est une première fois violé. D'autre part, le but réel d'utilisation des données n'ayant pas non plus été porté à la connaissance de la personne concernée, le juge constate en l'espèce la violation de l'article 4 de la loi.

5. Cette application de la règle de détermination des finalités, devrait, si elle est confirmée en appel, servir de mise en garde aux maîtres de fichiers, tous secteurs confondus. Le juge opte ici pour une application stricte de la règle, bannissant ainsi toute finalité énoncée de manière imprécise. On ne peut que s'en réjouir.

En l'espèce, il faut toutefois remarquer que le juge est ambigu sur le rôle joué par la banque. D'après lui, cette dernière agit en tant qu'assureur alors qu'elle n'intervient qu'en qualité d'intermédiaire d'assurance prospectant pour une entreprise d'assurance tierce. La différence est d'importance. Lorsque la banque agit en tant qu'assureur, elle le fait en tant qu'être juridiquement distinct de l'entreprise bancaire, conformément au jeu des articles 9 et 14 al. 3 de la loi du 9 juillet 1975 sur le contrôle des entreprises d'assurances. Une correcte application de l'article 1 par. 6 de la loi du 8 décembre 1992, pousse alors à distinguer deux maîtres du fichier différents. En effet, la décision relative au choix des finalités poursuivies ou des catégories de données traitées appartient respectivement à deux personnes morales distinctes, chacune pour ce qui la concerne : l'organisme bancaire proprement dit et l'organisme d'assurance émanant souvent du premier. Dans le contexte de la bancassurance, l'utilisation par l'assureur de données recueillies par le banquier implique alors une double finalité donnant lieu à deux traitements distincts dans le chef de deux maîtres du fichier : la finalité poursuivie par la banque consiste en une communication de données à un tiers dans un but de marketing, celle poursuivie par l'assureur en la promotion de ses propres produits.

Si par contre, comme c'est le cas dans le jugement commenté, la banque intervient en tant que courtier d'assurance, on conserve un maître du fichier unique, la banque, pour deux traitements distincts : le traitement relatif au marketing des produits financiers et celui relatif au marketing des produits d'assurance *d'autrui*.

## **2. Le contrôle de légitimité de la finalité : la finalité doit être légitime**

6. La légitimité d'une finalité est laissée, en règle générale, à l'appréciation des acteurs qui prennent part activement au processus de protection : le maître du fichier dans un premier temps, la personne concernée, la commission de protection de la vie privée et les juridictions judiciaires dans un second temps.

Le juge statue favorablement quant à la légitimité des finalités de marketing tant pour les produits financiers que pour ceux d'assurance. On se range volontiers derrière cette décision même si l'argumentation développée est un peu ténue.

La légitimité dépend directement d'un jugement de valeur quant à l'objet de la finalité. Il s'agit de savoir si le but poursuivi par le maître du fichier, dans le respect des règles protectrices, est acceptable dans une société dite démocratique, ce qui revient à pondérer les intérêts en présence. Le raisonnement est, à ce niveau, abstrait. L'intérêt du maître du fichier opposé aux libertés individuelles des individus justifie-t-il l'utilisation visée de données qui les concernent dans un but de marketing ? Le cadre du raisonnement pourrait être ici celui du principe de proportionnalité. L'intérêt invoqué implique-t-il une ingérence nécessaire et non-excessive dans le champ des libertés individuelles ?

7. Le marketing -spécialement le marketing direct- a pris dans l'activité économique d'aujourd'hui une importance capitale au niveau de la politique commerciale poursuivie par les entreprises. Il serait totalement irréaliste et vain de le rejeter en bloc sous prétexte de la protection de la vie privée des individus. Par contre, il est essentiel d'endiguer les excès auxquels il donne lieu et de contrôler les flux d'informations qui l'alimentent. Il faut toutefois bien comprendre de quoi il s'agit.

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"(7).

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(8).

Le marketing direct, quand il porte sur des personnes physiques, nécessite l'utilisation de listes de données d'identification 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 d'une opération publicitaire, soient soigneusement ciblés en fonction de caractéristiques qui leur sont propres (niveau de revenus, catégorie socio-professionnelle, lieu d'habitation 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(9).

Ce faisant, apparaissent différents traitements de données à caractère personnel qui tombent sous le champ d'application de la loi du 8 décembre 1992. Si la légitimité même de ces traitements ne pose généralement pas de problème, il faut encore déterminer quelles données peuvent être utilisées sans énerver la seconde règle du principe de finalité, dite de conformité des données(10).

### 3. Le contrôle de la conformité des données

8. Le principe de conformité des données exige que l'information soit pertinente, adéquate et non-excessive par rapport à la finalité poursuivie.

L'analyse du juge est assez tranchée, sans qu'une argumentation réelle ne soit développée. D'après lui, les données relatives aux nom et adresse du

destinataire, aux raisons du paiement et aux montants ne remplissent pas les conditions du principe de conformité tant pour la finalité de marketing des produits financiers que celui des produits d'assurances.

Quatre réflexions peuvent être faites relativement à cette position.

1) La décision du juge se limite au cas d'espèce. Il serait erroné d'y voir une interdiction de principe relative au traitement à des fins de marketing de toutes données générées par l'utilisation d'un moyen de paiement. Le juge statue ici sur la conformité des informations relatives au paiement d'une prime d'assurances à l'égard des deux finalités analysées. Ces informations particulières sont considérées comme ne présentant pas rapport avec la finalité de marketing de produits financiers puisqu'elles ne sont pas utilisées dans ce but et ne remplissent pas les conditions de pertinence et d'adéquation de l'information par rapport à la finalité réellement poursuivie, le marketing de produits d'assurance.

2) Le juge semble considérer certaines de ces informations comme excessives par rapport à la finalité de marketing des produits d'assurances. Il admet par contre expressément que "les informations relatives à l'identité du client doivent suffire à lui poser la question de savoir s'il est intéressé ou non par les activités de la banque comme assureur" (11).

Ainsi, le juge permet à la banque d'utiliser en bloc les données d'identification de sa clientèle bancaire pour le prospect des produits d'assurance. Remarquons qu'une action de marketing direct est peu réaliste sur cette seule base. Le but est précisément en cette matière de cibler au maximum les clients potentiels. Sans information pertinente permettant de catégoriser le public de référence, le marketing direct manque son but. Est-ce à dire qu'en l'espèce, tout ciblage est désormais exclu? Nous ne le pensons pas, mais il perdra sans doute en efficacité(12).

On bute ici sur une des questions essentielles posée par le marketing direct au vu du prescrit de la règle de conformité des données. La plupart des informations utilisées en marketing direct passent le cap des conditions d'adéquation et de pertinence : si une catégorie de données est employée c'est précisément parce qu'elle est utile et nécessaire au ciblage en cause. La logique économique rejoint ici celle de la protection recherchée. Toutefois, il arrive un moment où les catégories d'information deviennent excessives par rapport à la finalité du traitement; soit parce qu'elles donnent un profil trop complet des personnes en cause et provoquent un déséquilibre entre les intérêts en présence, soit, comme en l'espèce, parce que certaines catégories, dans leur singularité, provoquent en elles-mêmes ce déséquilibre. Le montant des primes d'assurance est exemplatif. L'information est très précieuse au niveau du ciblage : les personnes payant une prime plus élevée que le produit proposé présentent sans doute plus de chances d'être intéressés par un changement d'assureur. Toutefois, étant donnée la relation à la base de la commu-

nication de cette donnée à la banque, fondée sur la confiance réciproque, et l'ingérence du tiers banquier dans une relation contractuelle à laquelle il est étranger, il convient d'écarter cette donnée comme excessive en vue de la finalité de marketing-direct. Mais fallait-il pour autant rejeter toutes les données en cause ? Voilà sans doute une question à laquelle répondra la cour d'appel.

3) La question du caractère excessif des données en cause nous pousse à faire le lien avec un principe de protection absent comme tel de la loi du 8 décembre 1992 : celui de la loyauté de la collecte. L'article 5. a de la Convention n°108 du Conseil de l'Europe, à laquelle la loi est censée se conformer, exige que les données à caractère personnel soient obtenues et traitées loyalement(13). On ne trouve nulle part une explication claire des implications de ce principe. La loyauté est un de ces concepts flous au contenu indéterminé et évolutif, à l'instar de celui de la vie privée, de l'honnêteté en matière commerciale ou de la bonne foi en matière contractuelle. Elle renvoie tout à la fois au contexte qui entoure la collecte, à la finalité poursuivie et à la conformité des données. Utiliser une donnée à caractère personnel, sans en informer la personne concernée, sous le couvert d'un détournement de finalité, en violant la confiance légitime du client, nous paraît répondre à un acte de collecte déloyale au sens de la Convention.

4) Un argument intéressant soulevé par l'organisme bancaire était de prendre appui sur la recommandation n°R (90) 19 du Conseil de l'Europe relative à la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes(14). On sait que la commission de protection de la vie privée voit dans ces lignes directrices les standards internationaux auxquels doivent se référer les autorités et entreprises des Etats membres quand elles veillent à la correcte application des lois générales de protection(15). Les recommandations n'ont aucune force obligatoire dans l'ordre interne des Etats, ce qui permet à ceux-ci de s'éloigner, le cas échéant, des solutions retenues.

L'article 4.2. de la recommandation précitée admet expressément que les données liées à l'opération de paiement, collectées et enregistrées en vue de la gestion des moyens de paiement soient utilisées à des fins de marketing et de promotion de la gamme de services offerts. L'exposé des motifs précise qu'il faut entendre par là les services financiers ou autres proposés par la banque tels que l'organisation de voyage(16). Le courtage semble rentrer dans cette catégorie. Le juge admet ici la légitimité d'une utilisation des données pour l'offre d'un service d'assurance mais en limite fortement la portée *in casu* via l'application stricte du principe de conformité. S'il est vrai que des informations collectées en vue de la réalisation d'un service peuvent être utilisées dans l'offre d'autres services proposés, toute information ne peut être employée. C'est donc au cas par cas qu'il convient de raisonner. La limite à ne pas dépasser renvoie tant au *feeling* des acteurs garantissant la protection qu'à un sentiment collectif généralement partagé mais ne se laisse pas déterminer *a priori*, une fois pour toutes.



#### 4. Conclusion : la violation de la loi du 8 décembre 1992 comme acte contraire aux usages honnêtes en matière commerciale

9. Le juge qualifie les violations précitées de la loi du 8 décembre 1992 d'acte contraire aux usages honnêtes en matière commerciale, sur base de l'article 93 de la loi du 14 juillet 1991 relative aux pratiques du commerce.

Cet article vise spécifiquement l'atteinte ou la possibilité d'atteinte aux intérêts professionnels d'un ou de plusieurs autres vendeurs.

Le juge reste assez flou concernant la détermination de l'atteinte portée *in casu* aux courtiers par la seule violation de la loi du 8 décembre 1992.

D'après nous, cette atteinte ne consiste pas en l'utilisation d'informations inaccessibles aux courtiers. Il s'agit plutôt des conséquences de la mise en place de traitements de données à caractère personnel illégaux. Ces traitements illégaux permettent à la banque d'utiliser des informations qu'elle ne peut connaître dans la poursuite de la finalité de marketing de produits d'assurance.

Par là, le danger existe qu'en menant des campagnes de marketing plus ciblées, la société d'assurance liée s'octroie des parts de marché qu'elle ne pourrait conquérir en dehors de la violation de la loi et partant, que les autres courtiers voient, par répercussion, le montant global de leurs commissions s'amoinrir au profit de l'organisme bancaire. Telle paraît être l'atteinte virtuelle aux intérêts des courtiers.

10. L'analyse de la violation de la loi du 8 décembre 1992 en acte contraire aux usages honnêtes en matière commerciale pourrait bien être d'une aide précieuse aux autorités chargées de garantir l'application correcte de la législation protectrice.

Dans cette hypothèse, ce sont les maîtres du fichier eux-mêmes qui garantissent l'application de la loi par leurs pairs. On pouvait difficilement rêver d'un outil de contrôle plus efficace...

A la réflexion, deux types de violation de la loi du 8 décembre pourraient faire l'objet d'une action en cessation sur base de l'article 93 de la loi sur les pratiques du commerce.

La loi du 8 décembre 1992 met à charge des maîtres du fichier de lourdes obligations administratives dont la violation permet une utilisation plus efficace des données dans le chef de celui qui la commet. Dans cette hypothèse, la plus grande facilité de gestion se fait au détriment des autres maîtres du fichier qui, eux, sont censés respecter scrupuleusement le prescrit légal.

La loi interdit aussi l'utilisation de l'information qui se ferait en violant les libertés individuelles et les droits nouveaux reconnus à la personne concernée par les données.



Dans cette seconde hypothèse, c'est l'utilisation illégitime ou illégale d'une information exclue du traitement en cause qui donne alors au contrevenant un avantage potentiel sur les autres acteurs présents sur le marché.

Thierry LEONARD

Assistant à la faculté de droit de Namur (F.U.N.D.P.)

Chercheur au Centre de Recherche Informatique et Droit (C.R.I.D.)

Avocat au barreau de Bruxelles

(1) *Prés. 1e instance de Bruxelles, 22/3/1994, inédit relatif à un problème d'exactitude des données enregistrées par l'Union Professionnelle du Crédit; Prés. comm. Bruxelles, 15/9/1994, inédit relatif à un problème analogue à la décision commentée.*

(2) *Il faut toutefois souligner que le secteur bancaire est aussi celui qui paraît avoir été le plus actif en vue de l'application correcte de la loi. Sur les problèmes d'application de la loi dans le secteur bancaire, voir MEYSMANS, E., "Bancaire bestanden en privacy-bescherming in België", Computerrecht, 1992, n°1, 9; LEONARD, Th., "Banques et vie privée: deux problèmes d'application de la loi du 8 décembre 1992", in Droit de l'informatique: Enjeux – Nouvelles responsabilités, Bruxelles, éd. du Jeune Barreau de Bruxelles, 1993, 445 à 493; voir aussi les nombreuses contributions in Dossier n°46 de l'Association Belge des Banques, "La protection de la vie privée – La loi du 8 décembre 1992 relative au traitement de données à caractère personnel – Conséquences pour les banques", Bruxelles, A.B.B., avril 1993.*

(3) *Sur la portée de ces principes, voir LEONARD, Th. et POULLET, Y., "Les libertés comme fondement de la protection des données nominatives", in RIGAUX, F., La vie privée une liberté parmi les autres?, Travaux de la Faculté de droit de Namur n°17, Bruxelles, Larcier, 1992, 231 et svtes, spéc. 256 et svtes; GUTWIRTH, S., "De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens", T.P.R., 1993, 1409 et svtes, spéc. 1439 et svtes.*

(4) *L'article 16 par. 1er, 1° de la loi oblige le maître du fichier à tenir un état pour chaque traitement, contenant notamment le but du traitement. Une fois l'article 17 entré en vigueur, l'analyse de la finalité se fera principalement sur base de la déclaration du maître du fichier, quand elle est obligatoire.*

(5) *La version néerlandaise de la loi est plus explicite que la version française puisqu'elle parle de "(...) duidelijk omschreven en wettige doeleinden (...)".*

(6) *LEONARD, Th., "Banques et vie privée (...)", op. cit., 457, n°18 et svts.*

(7) *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.*

(8) *Pour plus de détails, voir WALTER, J.P., "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 XIIIe Conférence des Commissaires à la Protection des données (2-4 octobre 1991), Conseil de l'Europe, Strasbourg, 1992, 128 et 129.*

(9) *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, 14, n° 11). La recommandation régit principalement les listes de marketing direct sans apporter une réponse satisfaisante aux problèmes spécifiques à la mise en œuvre des fichiers de marketing. Pour une critique de cette approche, voir WALTER, J.P., op. cit., 147 et 148.

(10) Pour plus de détails sur le marketing direct dans le secteur bancaire et sur les problèmes qu'il pose, voir LEONARD, Th., "Banques et vie privée (...)", op. cit., 465 et svtes; Boone, A.D., "De nieuwe Belgische wet en de marketingactiviteiten van de banken", in Dossier n° 46 de l'Association Belge des Banques, 20 p.

(11) Traduction de l'auteur.

(12) La banque pourrait ainsi utiliser son fichier de difficultés de paiement pour ne proposer un nouveau produit d'assurance qu'à des personnes ayant les moyens financiers d'y faire face.

(13) Cfr la loi du 17 juin 1991 portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, M.B., 30/12/1993, 29023 et svtes.

(14) Recommandation n° R (90) 19, adoptée par le Comité des ministres du Conseil de l'Europe le 13 septembre 1990 et exposé des motifs, relative à la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes, Strasbourg, Ed. du Conseil de l'Europe, 1993.

(15) POULLET, Y., "Commercialisation des données détenues par le secteur public et vie privée", D.C.C.R., 1994, 609, n° 3.

(16) Recommandation n° R (90) 19, op. cit., 34, n° 56.