

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Le droit face aux nouvelles technologies bancaires

Schauss, Marc

Published in:
Les Informa-G-iciens

Publication date:
1986

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Schauss, M 1986, Le droit face aux nouvelles technologies bancaires. dans *Les Informa-G-iciens*. pp. 170-176.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

TROISIEMES JOURNEES DE REFLEXION SUR L'INFORMATIQUE

Les informa-g-iciens

Novembre 1986

Presses Universitaires de Namur

LE DROIT FACE AUX NOUVELLES TECHNOLOGIES BANCAIRES

Marc SCHAUSS

*Assistant au Centre de Recherches Informatique et Droit,
Facultés Universitaires Notre-Dame de la Paix - Namur*

C'est particulièrement dans son contact avec l'extérieur que l'informatisation du secteur bancaire suscite un questionnement, voire des inquiétudes au niveau juridique. Les services bancaires automatisés commercialisés se classent en deux grandes catégories, les services professionnels et ceux à vocation grand public.

Les applications professionnelles concernent tantôt les relations interbancaires, tantôt les relations entre la banque et l'entreprise. Les premières ont trait aux opérations de compensation (ex. : C.E.C. en Belgique), aux transferts de fonds (ex. : réseau international SWIFT) et à la gestion de titres (ex. : la centrale de livraison des valeurs immobilières CEDEL ayant son siège à Luxembourg). Les prestations offertes aux entreprises consistent principalement en des services d'information (ex. : cotes boursières, simulation de crédit, etc.) et de communication (ex. : consultation des comptes, ordres de paiement ou d'achat de titres).

Parmi les applications grand public, on relève les guichets automatiques de banque (permettant notamment le retrait ou le dépôt de billets), les terminaux points de vente (par exemple aux stations distributrices de carburant) et le "home banking" actuellement peu développé, lequel permet de bénéficier d'une série de services bancaires à domicile à partir d'un terminal relié à un ordinateur central par des lignes de télécommunications, généralement des lignes téléphoniques. Ces derniers services consistent en la fourniture d'informations financières et la possibilité d'effectuer des transferts de fonds impliquant ses propres comptes ou celui de tiers.

Le développement de ces nouveaux services regroupés sous le vocable "tebanking" conduit à se poser la question de leur réglementation et au-delà de cela, celle de l'adéquation du droit actuel au regard de techniques non imaginées par le législateur. Ces questions s'inscrivent dans le cadre

plus large des services télématiques en général ou, au contraire, dans un cadre spécifique à un type particulier d'application.

1. LES PROBLEMES ET LEURS SOURCES

Les discussions juridiques relatives aux diverses applications évoquées procèdent tantôt de caractéristiques essentielles à la technique mise en oeuvre, tantôt à des traits accidentels. Les éléments *essentiels* de la technique téléinformatique, générateurs de difficultés, sont la déshumanisation et la dématérialisation des opérations. Les traits *accidentels* résident dans la structure de l'offre des services, les conditions contractuelles qui les régissent et la multiplicité des personnes qui participent à l'opération.

La *déshumanisation* et la *dématérialisation* des opérations soulèvent certaines difficultés liées à la preuve des opérations, de leur réalité et de leur contenu. Dans nos pays, le papier et dans certains cas l'écrit signé, reçoivent de par la loi ou du fait de la culture juridique, un pouvoir de persuasion, une foi particulière. On relève à cet égard la recommandation du Conseil de l'Europe relative à l'admissibilité des enregistrements informatiques comme moyen de preuve (Recommandation N° R81(20) on the harmonisation on laws relating to the requirements of written proof and the admissibility of reproductions of documents and recordings on computers). Les problèmes de preuve entraînent des difficultés relatives aux responsabilités des acteurs (v. infra).

Ces caractéristiques essentielles des services "tebanking" sont communes aux services professionnels et grand public. Au sein du monde professionnel, certaines règles, notamment celles relatives à la preuve, sont différentes. Pour le reste, des solutions sont imaginées sous forme d'arrangements contractuels. De tels accords sont également formés entre les fournisseurs des services et les clients, qui s'appellent "règlement", "modalités d'utilisation", "conditions générales", ou plus simplement "contrat". Mais, alors qu'ils ne semblent pas faire difficulté dans le monde professionnel, ils suscitent des questions s'agissant du grand public. Celles-ci trouvent leur source dans la structure de l'offre, le contenu des modalités prévues par les contrats et la multiplicité des intervenants.

La *structure de l'offre* des services tebanking se caractérise par la politique commerciale des institutions financières qui cherchent à diffuser largement certains services, particulièrement ceux relatifs au paiement par carte magnétique, lesquels comportent des risques techniques non encore résolus et exigent des investissements importants. Ce dernier élément explique la tendance à la concentration des moyens qui s'accompagne généralement d'une standardisation des conditions d'utilisation des services proposés. Celles-ci sont parfois *déséquilibrées* au détriment de l'utilisateur, ce qui inquiète certaines organisations de consommateurs. Enfin, la *multiplicité des acteurs* participant à l'opération (banque gérant le compte

du client, banque ou propriétaire du lieu où est situé le terminal, utilisateur, bénéficiaire, société de services techniques, administration ou entreprise de télécommunications, etc.) rend aigu le problème de la détermination des responsabilités.

Des actions ont été entreprises (ex. : loi américaine de 1978; loi danoise de 1984) ou sont à l'étude (ex.: Rapport du Conseil National de Crédit français sur les nouveaux moyens de paiement de juillet 1986; recommandations de la commission fédérale suisse de la consommation de février 1986; avant-projet d'articles concernant l'émission et l'utilisation des cartes de crédit, des cartes de paiement et des cartes multifonctions de la DG XI de la Commission des Communautés Européennes de 1986) qui visent notamment à réaliser un partage acceptable des avantages des nouveaux moyens de paiement entre les différentes parties intéressées.

2. LE DIFFICILE EQUILIBRE : DE CERTAINS CHOIX

Les discussions portent sur l'équilibre entre certains intérêts à protéger. Ces intérêts sont le développement d'un marché européen par la promotion des facilités de paiement particulièrement sous un angle international, l'équilibre contractuel, la prévention des conflits, la sécurité des transactions et la protection de données à caractère personnel.

La *promotion* des services de paiement électronique risque d'avoir des conséquences néfastes. D'une part, l'offre massive de ce type de services conjuguée à son acceptation par le public peut porter atteinte à la concurrence entre procédés de paiement. Or, certaines personnes peuvent préférer d'autres procédés pour des raisons diverses tels par exemple le souci de conserver l'anonymat, la crainte de devoir mémoriser un code, celle d'être victime de fraudes, le désir d'être modéré dans les dépenses par la sensation d'appauvrissement que procure le paiement par argent liquide ou enfin l'appréhension de négligence vis-à-vis de documents à valeur dérivée (telle la carte magnétique).

L'*internationalisation* des services telebanking suppose une normalisation technique qui, alliée à la tendance concentrationniste due à l'ampleur des investissements, risque de réduire la structure concurrentielle de l'offre desdits services. Par contre, l'interbancaire des moyens d'accès aux services (ex. : carte magnétique) diminue le risque de clientèles captives d'un fournisseur utilisant une technique spécifique incompatible avec celle utilisée par les concurrents.

Actuellement, certaines clauses sont trop désavantageuses pour l'utilisateur. La situation de *déséquilibre* procède particulièrement du fait que c'est le fournisseur du service qui, d'une part, a la maîtrise quasi-totale de la technique et, d'autre part, détient les moyens de preuve (ex. les

"login") dont l'utilisateur pourrait avoir besoin. Ce déséquilibre est accentué par certaines clauses contractuelles. On songe notamment aux modalités de modification et de fin du contrat à l'avantage exclusif de l'organisme financier, à la convention de preuve qui prévoit que la bande journal fait preuve entre les parties alors que seule l'une d'elles a la maîtrise de sa rédaction ou, encore, au régime de responsabilités (les clauses sont quelquefois peu clairement rédigées, parfois interprétées sévèrement du point de vue de l'utilisateur et généralement conçues à l'avantage du fournisseur telle par exemple la clause qui impose à l'utilisateur la conservation du caractère confidentiel du code d'accès - ce qui est indispensable pour le bon fonctionnement du système - sans mettre à charge de l'organisme financier une obligation corollaire de vigilance dans la génération, la communication et la gestion de ce code). Afin de rétablir le déséquilibre, un courant doctrinal se montre favorable à mettre à la charge de l'établissement financier une présomption de responsabilité jusqu'à plus ample informé. En réalité, établir une présomption ne résout rien si la situation de la partie que l'on entend protéger est toujours aussi fragile une fois la présomption renversée. Or, renverser une présomption n'est pas problématique lorsqu'on dispose de moyens de preuve auxquels le juge accorde une foi suffisante. Ce qui est important, c'est la possibilité pour l'utilisateur de se ménager les moyens de preuve détenus par un tiers. C'est la solution de la loi américaine et de la récente proposition du Conseil National du Crédit français. Notons que le problème de la preuve ne se pose pas uniquement pour l'utilisateur, mais aussi pour l'organisme financier. Aussi, prévenir la négligence du client apparaît nécessaire.

Régler les contentieux de manière souple est certes une des missions des juristes. Mais rien ne vaut la *prévention* des litiges. Or, le sentiment d'insatisfaction que peut avoir l'utilisateur, à la suite d'erreurs et les moyens juridiques inadéquats au regard de la technique utilisée, peuvent conduire à des procès coûteux (frais d'expertise par exemple) et aléatoires. Outre la tentative de limitation des sources d'insatisfaction des parties par le rétablissement d'un équilibre contractuel, il convient de réglementer les pratiques antérieures à la conclusion du contrat d'utilisation des services telebanking. Une des exigences fondamentales de la période pré-contractuelle réside dans l'information du futur utilisateur relativement à l'objet du service, à l'identification du responsable, aux responsabilités, à la procédure de règlement de conflit, au coût, aux modalités de modification et de fin de contrat et aux informations à caractère personnel récoltées, stockées, traitées et communiquées à des tiers. Les lois américaine et danoise prêtent une grande attention à l'information du client. Un autre procédé de prévention des litiges est mis en place par la loi danoise. Celle-ci prévoit un contrôle a priori de qualités minimales du service par l'Ombudsman. Enfin, on a relevé supra que les règles de preuve entraînaient des difficultés s'agissant de déterminer les responsabilités. Si la preuve d'un éventuel dommage n'est pas problématique, il n'en va pas de même de celle de sa cause et de son imputabilité. Aussi s'oriente-t-on vers une responsabilité objective, fondée non plus sur le critère traditionnel de

la faute mais sur un partage a priori des risques. Dans ce système, l'utilisateur prendrait en charge les risques antérieurs à la déclaration d'erreur et le fournisseur, ceux postérieurs à cette notification. La solution belge (décision de la Cour d'appel de Liège du 22 février 1985, in *Droit de l'Informatique*, 1985, n° 6, p. 28, note B. Amory) est assez proche de cette construction. Celle-ci risque toutefois de faire l'objet de réticences de la part des fournisseurs de services telebanking disposant de systèmes off-line. En l'occurrence, le droit exige l'adaptation des techniques utilisées dans les systèmes mis à la disposition du public.

La *sécurité des transactions* suppose que soient minimisées les fraudes. Or, les techniques téléinformatiques mises en œuvre actuellement n'offrent pas des garanties de sécurité et les comportements de certaines personnes suscitent les inquiétudes de toutes les parties intéressées. Il est certain que les perfectionnements techniques constituent la meilleure voie de résolution du problème. On note à cet égard l'action des Communautés Européennes (ex. projet OSIS mené dans le cadre du programme européen COST). Certaines normes déontologiques sont efficaces également. Enfin, l'élaboration de normes pénales visant à réprimer les fraudes informatiques et télématiques est actuellement en voie d'élaboration ou à l'étude dans plusieurs Etats et organisations internationales, notamment l'OCDE.

Enfin, la problématique de la *protection des données à caractère personnel* met en jeu de multiples intérêts en sens divers. Le premier auquel on songe est évidemment celui du client dont on pourrait dégager le profil de consommation, les habitudes de déplacements et les heures de présence à domicile. Ces informations peuvent affecter la liberté de l'utilisateur d'obtenir du crédit, ainsi que sa liberté d'opinion et d'action. D'autre part, la collecte et le traitement de certaines de ces informations présente un double intérêt pour l'utilisateur. En effet, la mémorisation de certaines données constitue une trace de l'opération qui pourrait servir de preuve en cas de litige et leur traitement peut, dans certains cas, être avantageux pour le client (ex. le relevé des achats de carburant en fin de mois pourrait être étendu à d'autres marchandises et constituer une comptabilité analytique domestique). La collecte de certaines informations représente un intérêt pour le fournisseur du service et le commerçant chez qui un terminal point de vente est installé. Ils pourraient, par cette voie, avoir une meilleure connaissance de leur clientèle, disposer d'une comptabilité analytique complète, gérer les stocks et les achats et se ménager des preuves en cas de difficulté. Enfin, l'administration et le juge trouveront un intérêt à la communication de certaines informations leur permettant d'accomplir leur mission plus efficacement. On le voit, les intérêts en jeu sont multiples et parfois opposés. Les réglementations actuelles relatives à la protection des données à caractère personnel se sont surtout centrées sur les informations créées a priori, c'est-à-dire antérieurement à la mise en œuvre d'un service alors que le danger que présentent les services telebanking provient essentiellement de données a posteriori, c'est-à-dire créées lors de et par la consommation du service.

Tout le monde s'accorde à reconnaître l'importance du problème et l'insuffisance des réglementations en vigueur.

3. VERS UNE REGLEMENTATION EUROPEENNE ?

La question est double : celle de la pertinence d'une réglementation et celle de son éventuelle vocation européenne.

La loi américaine, la première à avoir réglé spécifiquement certains aspects importants du problème, a été critiquée comme étant prématurée dans l'état d'évaluation des implications. Les réglementations destinées à accompagner le développement technologique encourent le double risque de devenir rapidement obsolètes et de déplacer les difficultés, en supprimant certaines et en générant de nouvelles. Il s'agit donc d'évaluer la pertinence et le degré d'urgence d'une *éventuelle réglementation* et d'en mesurer les avantages et les coûts. Ceci implique une étude du cadre de la problématique, des effets souhaités ainsi que de l'extension des concepts juridiques intégrés dans les réglementations actuelles afin d'en tirer parti au mieux (principe de continuité des normes). La traduction des valeurs à promouvoir sous forme de normes implique une maîtrise des concepts nouveaux à mettre en œuvre et de leur champ d'application. Aussi des études sont-elles menées un peu partout en Europe et en Amérique du Nord (ex. action du SPPS, programmes FAST et Legal Observatory de la DG XIII de la CEE ; étude du Conseil National du Crédit français, etc.).

L'élaboration de réglementations nationales risque de créer des distorsions affectant le commerce entre Etats membres de la CEE. On songe particulièrement aux mesures protectrices des consommateurs et des données à caractère personnel mais aussi au régime des responsabilités et à la répression des fraudes. Aussi s'accorde-t-on à reconnaître la nécessité d'une *réglementation internationale* d'autant plus que la problématique est récente et que les traditionnelles résistances nationales seraient vraisemblablement peu importantes vu l'absence de réglementation dans la plupart des pays. C'est dans cette perspective que doivent être comprises les différentes actions des organisations internationales relatives à la problématique (ex.: actions précitées des Communautés européennes, recommandation du Conseil de l'Europe en matière de preuve au moyen d'enregistrements informatiques, études de l'OCDE particulièrement s'agissant de la fraude informatique, études de la Commission des Nations-Unies pour le Droit Commercial International, etc.).

4. BIBLIOGRAPHIE

- *Electronic Fund Transfer Act* (Etats-Unis).
- *Lov om betalingskort* (Loi danoise n° 286 du 6 janvier 1984).
- Conseil National du Crédit, *Rapport du groupe de travail sur les aspects juridiques des nouveaux moyens de paiement*, Paris, juillet 1986.
- Revue *Droit de l'informatique*, 1986/3, Dossier monétique.
- *La Télématique*, Actes du colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit (C.R.I.D.) des Facultés Universitaires Notre-Dame de Namur, Story-Scientia, Gent, 1985, tome II, Chapitre V.