CAHIERS AEDBF/EVBFR-BELGIUM

— 13 —

TRANSFERTS ÉLECTRONIQUES DE FONDS LES PAIEMENTS PAR WAP

Actes des journées d'études le 18 novembre 1999
et le 5 octobre 2000 organisé par
l'Association Luxembourgeoise des juristes de banque,
le Centre de Recherches Informatique et Droit (CRID)
la Faculté de Droit de Namur et l'Association Européenne
pour le Droit Bancaire et Financier-Belgium
(AEDBF-Belgium)

EXTRAIT

BRUYLANT
BRUXELLES

2 0 0 1

OBSERVATIONS INTRODUCTIVES AU COLLOQUE SUR LES TRANSFERTS ÉLECTRONIQUES DE FONDS

PAR

André PRÜM

PROFESSEUR À LA FACULTÉ DE DROIT DE NANCY (*)

(*) Directeur du Centre de Recherche de Droit Privé de l'Université de Nancy 2 et du Laboratoire de Droit Economique du Centre de Recherche Public Gabriel Lippmann à Luxembourg.

Au sens le plus général, les transferts électroniques de fonds embrassent l'ensemble des moyens qui permettent de réaliser un transfert monétaire sans s'appuyer sur un ordre ou un titre en papier. La catégorie s'étend ainsi d'opérations classiques, tels les virements électroniques ou les effets de commerce dématérialisés, aux cartes à puce chargées d'unités monétaires ou autres « portes-monnaie virtuels ».

Leur développement aussi bien que la recherche de solutions innovantes se trouvent aujourd'hui fortement stimulés par l'essor du commerce électronique. S'accomplissant à travers des transactions conclues sur le réseau Internet, celui-ci suppose des techniques de payement utilisables « *en ligne* ». Les solutions permettant de répondre à cet impératif varient du simple usage d'une carte de payement ou de crédit aux applications les plus sophistiquées reposant sur l'utilisation de « monnaies électroniques » (1).

Moyens ou véritables instruments de payement, ces techniques présentent des fonctionnalités aussi bien que des niveaux de sécurité différents et s'appuient sur des architectures contractuelles originales (I). Leur emploi soulève de nombreuses questions juridiques sur lesquelles le présent exposé introductif se propose modestement d'ouvrir le débat (II).

I. — Aperçu des techniques de payement « *en ligne* »

A l'heure actuelle, le payement de la plupart des transactions conclues sur le réseau Internet s'effectue par le biais d'instructions données au moyen d'une simple communication des références visibles — numéro et date d'expiration — d'une carte de payement ou de crédit. Sans prendre certaines précautions, la pratique présente de toute évidence des risques importants aussi bien pour l'accipiens que pour le titulaire de la carte. Le premier s'expose, en effet, au danger de voir son

(1) Pour une description technique, cf. l'ouvrage de H. Sherif et Serhrouchni, *Monnaie électronique*, Paris, Eyrolles, 1999.

débiteur renier tout ordre de payement alors qu'il n'a pas présenté physiquement sa carte ni soumis celle-ci à un quelconque contrôle à distance. Quant au titulaire de la carte, qui accepte d'en fournir les références sur le réseau Internet, il prend le risque à la fois de les adresser directement à un correspondant malhonnête et d'en permettre l'interception par un tiers indélicat qui, l'un ou l'autre, pourraient s'en servir frauduleusement par la suite.

Afin de se prémunir contre ces dangers, diverses solutions ont été développées pour permettre une utilisation plus sûre des cartes de payement sur l'Internet (A). En parallèle, de nouvelles techniques, indépendantes des moyens de payement classiques, ont été conçues. Leur trait commun est de chercher à offrir aux utilisateurs les fonctionnalités d'une véritable « monnaie électronique », sans en épouser cependant nécessairement les caractères (B).

A. — *L'adaptation des techniques de payement classiques au commerce électronique*

La précaution élémentaire à prendre avant de donner une instruction de payement sur l'Internet au moyen d'une carte est de se protéger des écoutes indésirées en rendant illisibles, par la voie d'un chiffrement ou cryptage, les références de la carte au moment où celles-ci transitent par le réseau. Les correspondants doivent utiliser à cette fin une voie de communication sécurisée par une clef commune (ou symétrique) qu'ils se partage pour crypter et décrypter les messages échangés. Le protocole le plus répandu est le « *Secure Socket Layer* » (SSL), développé par la société Netscape en collaboration notamment avec Mastercard (2). Il présente l'avantage d'être intégré dans les outils communs de navigation sur l'Internet. Son niveau de sécurité demeure toutefois actuellement limité en raison de la taille modeste de la clef de chiffrement sur laquelle il s'appuie. La protection ne s'applique de surcroît qu'à la seule phase du transport des données et ne met, par conséquent, pas le titulaire de la carte à l'abri d'un piratage des données sur le serveur du commerçant auquel il les aura communiquées.

(2) http://www.sslhosting.com.

Prémunissant les correspondants contre les regards extérieurs indiscrets, l'échange de données cryptées ne leur donne, en soi, aucune assurance sur leurs identités respectives. Or, sur un réseau où les présences restent purement virtuelles, le danger de rentrer en contact avec un correspondant malhonnête, voire de véritables escrocs reste loin d'être hypothétique. Avant de communiquer les références de sa carte bancaire sur un site Internet, son titulaire sera dès lors bien avisé de s'assurer que le propriétaire du site est effectivement la personne à laquelle il pense s'adresser (3). De même, le commerçant, qui entend se prémunir contre les clients qui refuseraient de payer des commandes passées en ligne, aura tout intérêt à obtenir des renseignements sur leur identité ainsi qu'une confirmation de leurs ordres de payement. L'utilisation de signatures électroniques associées à des certificats émanant d'autorités indépendantes attestant le lien entre le dispositif utilisé pour vérifier les messages signés et l'identité de celui qui s'en prévaut, permet de lever ces inquiétudes.

Pour les payements en ligne reposant sur l'utilisation d'une carte de crédit, ces fonctionnalités sont susceptibles d'être remplies par le protocole « *Secure Electronic Transaction* » (SET) développé par les sociétés Mastercard et Visa (4). Reposant sur la technologie de la cryptographie asymétrique, permettant une certification des signatures, le dispositif assure à la fois l'identification des parties à la transaction, l'intégrité de la communication et une protection contre la remise en cause des instructions de payement. Une variante de ce système a récemment vu le jour en France pour les cartes à puces dont le code confidentiel peut avantageusement être vérifié grâce à un lecteur spécifique connecté à l'ordinateur de son titulaire (« *Chip Secure Electronic Transaction* », C-SET) ou intégré dans son téléphone mobile.

Le niveau de sécurité élevé de SET au regard des standards actuels induit une certaine lenteur des transactions aussi bien qu'un renchérissement de leur coût, sensibles surtout pour les payements de valeur modique. Au surplus, il n'autorise pas

(3) La version 3 du protocole SSL intègre une authentification obligatoire des sites commerciaux.

(4) http://www.setco.org

une utilisation anonyme des cartes de payement, ce qui est de nature à décourager ceux qui souhaitent pouvoir réaliser leurs achats sur Internet sans devoir systématiquement révéler leur identité, comme ils peuvent légitimement le faire dans le commerce traditionnel en se servant de billets et de pièces. Bien qu'opérationnelle, la solution n'a, pour ces raisons, pas encore su s'implanter à large échelle.

Une alternative économique au système SET, spécialement adaptée aux micro-payements, consiste à substituer à l'utilisation des références d'une carte de payement ou de crédit l'emploi d'un code convenu entre le titulaire et un créancier habituel. La solution est préconisée par certains sites grand public (tels amazon.com ...) qui proposent cette facilité à leurs clients après avoir récupéré, par un moyen de communication traditionnel (courrier, téléphone ou télécopie), les coordonnées de leurs cartes avec un engagement formel de leur part d'honorer les achats. Protégeant les clients contre une interception frauduleuse des références de leurs cartes par des tiers, la méthode suppose évidemment une grande confiance dans le commerçant. Elle demeure de ce fait confinée à des relations particulières et n'est pas susceptible de s'étendre aux paiements auprès d'autres commerçants.

A la fois plus ouverts et plus sûrs apparaissent à cet égard les mécanismes faisant intervenir un tiers habilité à conserver les références de cartes de payement ou de crédit et chargé, après vérification des instructions de payement émanant d'un titulaire, de transmettre celles-ci à la banque émettrice en confirmant, le cas échant, le payement au créancier. Divers projets reposant sur une telle intermédiation ont déjà vu le jour (Cybercash (5), Payline (6), First Virtual (7)...). La plupart supposent de la part du titulaire de la carte qu'il protège (par un chiffrement) tout ou partie des instructions de payement communiquées à son créancier afin d'empêcher celui-ci d'en prendre directement connaissance et de l'obliger ainsi à les faire valider par l'intermédiaire disposant des clefs de déchiffrement nécessaires. Une variante de ce système, sous la

(5) www.cybercash.com
(6) www.payline.com
(7) Arrêté en 1998.

forme de la création d'une représentation logicielle de la carte (e-card), est actuellement à l'étude par un vaste consortium comprenant aussi bien les principaux gestionnaires de cartes que de grandes entreprises informatiques. L'objectif affiché par le projet est de mettre à la disposition des titulaires un fichier sécurisé contenant les références de leurs cartes grâce auquel ils pourraient donner des instructions de payement sans être exposés aux risques de fraude perpétrés par des tiers ou des commerçants créanciers.

Signalons enfin que parallèlement aux efforts déployés pour améliorer la sécurité des payements reposant sur l'utilisation d'une carte, d'autres voies ont été imaginées sur la base du chèque. La perspective n'est plus toutefois d'adapter cet instrument classique au commerce en ligne mais de concevoir l'équivalent numérique du chèque sur support papier (E-check (8), Virtualcheck (9)). Aussi, s'agit-il plutôt de modalités particulières des virements électroniques et non de la création de titres soumis à la réglementation des chèques.

B. — *A la recherche de nouveaux instruments de payement : l'avènement d'une « monnaie électronique »?*

Cherchant à imiter les caractéristiques des pièces et des billets, les premières illustrations de monnaies dites « *électroniques* » ont cherché refuge dans des supports physiques classiques, typiquement une puce électronique apposée sur une carte de payement (« *cartes intelligentes* » ou « *smart cards* »). Plus récemment, de nouvelles formes de ces « *monnaies* » se sont contentées d'expressions purement électroniques.

1. *La solution « hardware » des « cartes intelligentes » (« smart cards »)*

Si le chargement de l'équivalent d'une certaine somme d'argent sur une carte à puce utilisable auprès d'un commerçant déterminé n'est pas une invention récente (Cf. par exemple les cartes téléphoniques ...), le développement de cartes à

(8) www.e-check.com, cf. aussi www.acceleratedpayment.com
(9) www.virtualcheck.com

vocation universelle repose sur des solutions technologiques aussi bien qu'opérationnelles entièrement nouvelles. Les applications les plus connues à ce jour sont celles des cartes Visacash (10), Geldkarte, Mondex (11), Proton (12), Monéo, Modeus et Internet Cash (13). Elles sont destinées aussi bien aux payements de faible valeur dans le commerce de proximité qu'aux règlements sur Internet.

Émises par des établissements de crédit ou de grands réseaux des cartes traditionnelles, elles se présentent sous la forme d'instruments incorporant d'office une valeur déterminée, insusceptible d'être modifiée (« cartes prépayées »), ou de cartes librement rechargeables par leur titulaire par débit de leur compte auprès de l'émetteur. À chaque utilisation, la carte se trouve ensuite déchargée du montant de la transaction qui est crédité sur le dispositif de lecture du créancier. À la différence de l'emploi d'une carte de payement ordinaire, l'opération s'effectue normalement sans l'indication d'aucun code secret, ni d'aucune signature. Aboutissant à un transfert définitif d'une certaine quantité de « *monnaie électronique* », le payement est, en principe, libératoire pour le solvens. En fonction des systèmes, l'accipiens devra par la suite requérir la conversion de la valeur chargée en monnaie scripturale auprès de l'émetteur ou pourra la réutiliser librement pour un nouveau payement auprès d'une autre personne acceptant cette « monnaie électronique » (14).

2. *La solution « software » : la monnaie virtuelle*

Dans les solutions purement électroniques, dessinées spécialement pour les payements sur Internet, la carte intelligente comme support de la valeur se trouve remplacée par un programme informatique, communément désigné « *porte-monnaie électronique* ou *virtuel* ». Le principe a été retenu par des applications comme Cybercoin de Cybercash (15), e-cash de Digicash (16), Netbill (17), BarclayCoin, Kleline (18) ou PayPal (19).

(10) www.visa.com
(11) www.mondex.com
(12) www.Banksys.be ; www.Protonworld.com ; www.cartes-bancaires.com
(13) InternetCash.com
(14) C'est le cas du système Mondex.
(15) www.cybercash.com

L'alimentation du « *porte-monnaie virtuel* » s'effectue par une procédure en ligne par laquelle le titulaire demande à sa banque de lui fournir l'équivalent d'une somme d'argent déterminée en pièces ou jetons électroniques identifiés par un numéro de série et protégés contre toute falsification. Alternativement, ces pièces peuvent également être générés par le porte-monnaie du titulaire qui les soumet ensuite à une validation auprès de sa banque. Cette dernière solution présente l'avantage de procurer au titulaire un moyen de payement anonyme dont il pourra se servir sans permettre à la banque de retracer l'utilisation des pièces utilisées (20).

Une fois chargé, le titulaire du « *porte-monnaie virtuel* » peut ensuite se servir des pièces en les adressant, par voie électronique à un créancier disposant du logiciel nécessaire pour les recevoir. Chaque transfert donne lieu, en principe, à une vérification en ligne des pièces utilisées auprès de la banque émettrice qui contrôlera, en particulier, si celles-ci sont toujours valides et n'ont pas déjà servi à un autre payement. En fonction des systèmes, les pièces transférées se trouvent alors soit définitivement éteintes et doivent être converties en monnaie scripturale, soit peuvent être réutilisées.

La procédure de validation pouvant s'avérer trop lourde et, par conséquent, trop onéreuse pour les micro-payements, la société Millicent (21) a conçu une solution alternative dans laquelle les pièces — dénommés « *scripts* » — sont vérifiées directement par le commerçant qui les accepte comme mode de paiement. En contre-partie, ces « *scripts* », ne sont utilisables qu'auprès d'un commerçant déterminé ou du courtier auprès duquel le client se les a procurés.

(16) www.digicash.com
(17) www.netbill.com
(18) www.kleline.com (projet abandonné à la suite de la fusion entre la BNP et Paribas).
(19) PayPal.com
(20) Solution préconisée par e-cash.
(21) www.millicent.com

II. — Interrogations soulevées par les techniques des payement « *en ligne* »

Dans une démarche purement pragmatique, sans prétention théorique, les principaux risques des différentes techniques utilisées pour les payements « *en ligne* » apparaissent être à la fois d'ordre patrimonial, systémique et social.

A. — *Les risques patrimoniaux*

Cette première catégorie s'entend de tous les dangers de perte ou de responsabilité que les instruments et moyens de payement susceptibles d'être utilisés « *en ligne* » font courir au solvens et à l'accipiens comme à l'émetteur et à tous ceux qui contribuent, à un titre ou un autre, à leur gestion.

Les risques sont liés à des circonstances variées mais bien connues tenant, en particulier, à l'absence de provision ou de couverture du moyen de payement, à sa perte ou sa destruction, liées notamment à une défaillance du support, à son utilisation frauduleuse par un tiers non autorisé, à l'insolvabilité du teneur de compte ou de l'émetteur de l'instrument de paiement ou la défaillance du gestionnaire du système de paiement...

Les relations contractuelles qui sous-tendent les différents instruments ou moyens de payement s'emploient à distribuer ces risques. En pratique, la charge en incombe le plus souvent principalement aux titulaires ou porteurs et, en seconde ligne, aux commerçants acceptant ces modes de payement. Le partage ne semble d'ailleurs pas toujours conforme aux prescriptions du droit communautaire (22).

Mais surtout, ces arrangements conventionnels ne sauraient plus longtemps faire l'économie d'une analyse de la nature exacte des instruments ou moyens de payements auxquels ils s'appliquent et des effets qui en découlent pour les parties. Or,

(22) Cf. en particulier la Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, article 8 et la proposition de directive concernant la commercialisation à distance de services financiers auprès des consommateurs qui dans sa mouture du 29 octobre 1999 prévoit une disposition équivalente ainsi que la Recommandation 97/489/CE de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire.

une différence profonde semble exister, à cet égard, entre l'utilisation, même selon des procédés sécurisés, des cartes de paiements traditionnelles et l'emploi des nouvelles formes de « *monnaie électronique* ».

S'agissant des premières, elles servent simplement à leur titulaire à donner une instruction de payement à l'émetteur, qui en soi n'opère pas celui-ci mais constitue uniquement un acte préparatoire au payement. Il s'ensuit que le créancier qui se contente d'une telle instruction court le risque de ne pas être payé en cas de couverture insuffisante du compte du titulaire de la carte, du moins au delà de la garantie que lui offre la banque. Lorsque qu'au surplus l'instruction de paiement a été donnée sans présentation physique, ni vérification électronique de la carte, le commerçant s'expose également au danger de voir son client renier purement et simplement l'existence même de cette instruction. Inhérent à la nature de ces moyens de paiement, par opposition aux véritables instruments, le risque d'un transfert non autorisé ou contesté par le titulaire de la carte est susceptible de peser, par ailleurs, sur la banque émettrice.

Il en va *a priori* tout autrement en cas d'utilisation d'une « monnaie électronique ». Quelle que soit la qualification juridique qu'il convient de reconnaître aux unités de valeur stockées sur une carte intelligente ou dans un porte-monnaie virtuel — monnaie, substitut de monnaie ou droit de créance d'une autre nature (23) — il convient d'observer, en effet, que les droits du titulaire de cette « monnaie » se trouvent ici, détachés de toute relation de compte. Celui-ci n'en devient-il pas alors personnellement gardien de sorte qu'il devrait assumer seul et intégralement les suites d'une perte, d'un vol ou d'une utilisation frauduleuse de cette monnaie? Il serait également logique d'admettre dans ce cas que le transfert à un tiers créancier emporte libération immédiate du solvens. Ce qui signifierait que l'émetteur se trouverait dorénavant personnellement tenu vis à vis de l'accipiens, engagement qui comporterait l'obliga-

(23) Voir à cet égard la définition hybride retenue par la directive 2000/46 du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements dans son article 1er, 3e alinéa et le 3e considérant.

tion de convertir les unités monétaires acquises en monnaie scripturale ou fiduciaire. Le risque essentiel auquel ce dernier pourrait dès lors se trouver exposé ne serait plus celui d'un défaut de provision du compte de son débiteur, mais celui d'une éventuelle insolvabilité de l'émetteur. Ce danger existerait également pour le titulaire tant qu'il n'a pas dépensé la « *monnaie électronique* » chargée sur sa carte ou dans son porte-monnaie virtuel dans la mesure où il pourrait prétendre lui-même à un remboursement de la part de l'émetteur (24). La question de savoir si l'un et l'autre pourraient bénéficier, le cas échéant, de la garantie obligatoire des dépôts (25), ne semble pas encore résolue. Pas plus que ne l'est celle du statut et de la propriété des réserves constituées en couverture de l'émission de « *monnaie électronique* » (existence d'un droit de revendication du titulaire de la monnaie, saisisabilité par des tiers...).

Une chose est certaine, les hésitations levées par de telles divergence ne permettent plus d'envisager le partage des risques patrimoniaux pour les payements accomplis en « *monnaie électronique* » de la même façon que pour les instructions de payement données au moyen d'une carte.

B. — *Les risques systémiques*

L'avènement des nouvelles techniques de paiement électronique, en particulier les diverses figures de « *monnaie électronique* », recèle de toute évidence certains risques pour le système monétaire et financier pris dans son ensemble.

Le premier enjeu, qui concerne tout aussi bien la solidité du système que la position concurrentielle de ses principaux acteurs, a trait au statut de ceux qui sont autorisés à émettre les nouvelles formes de « *monnaie électronique* ». Il vient de trouver une réponse dans deux directives du 18 septembre 2000 élargissant la notion d'établissement de crédit (26) et réglementant l'accès à l'activité des établissements de monnaie

(24) Tel que le prévoit la directive 2000/46 du 18 septembre 2000, précitée dans son article 3.

(25) Directive 94/19/CE du Parlement Européen et du Conseil, du 16 mai 1994 relative aux systèmes de garantie des dépôts (*JOCE*, L 135, 31.5.94).

(26) Directive 2000/28/CE publiée au *JOCE*, L 275/37 du 27 octobre 2000.

électronique et son exercice (27) qui, outre les établissements de crédit, réservent cette émission à une nouvelle catégorie d'entreprises, « *les établissements de monnaie électronique* ». Dérogeant au traditionnel monopole des banques, cette nouvelle réglementation limite cependant strictement l'activité des établissements en question en les soumettant, entre autres, à l'obligation d'obtenir un agrément et le respect d'exigences prudentielles adaptées aux risques qui leur sont propres.

Le développement de « *monnaies électroniques* » susceptibles de se substituer, même temporairement, aux expressions fiduciaires ou scripturales pourrait, par ailleurs, avoir un impact sur contrôle de la masse monétaire (28) et entraîner une diminution de la quantité de billets et de pièces en circulation, privant le cas échéant, les Banques centrales des revenus importants tirés de leur droit de seigneurage (29).

C. — *Les risques sociaux*

L'ensemble des techniques de payement envisagées se caractérise par une gestion quasi totalement informatisée. L'on voit poindre immédiatement dans cette dépendance le spectre des dangers que la puissance de calcul des ordinateurs traitant des données nominatives fait peser sur la vie privée des citoyens. A de rares exceptions près, les moyens et instruments considérés ne se soucient, en effet, guère de la confidentialité des transactions. Si le risque n'est évidement pas propre aux payements « *en ligne* », il pourrait cependant s'avérer en l'espèce d'autant plus critique que les données circulant sur l'Internet deviennent potentiellement accessibles à un nombre illimité de personnes et qu'au surplus elles pourront facilement être associées à d'autres renseignements personnels permettant ainsi la création de profils de consommation ou d'épargne extrêmement précis. Afin de se prémunir contre de telles atteintes, les utilisateurs seront sans doute enclins à privilégier l'usage de

(27) Directive 2000/46/CE, publiée eu *JOCE*, L 275/39 du 27 octobre 2000.

(28) Pour une description plus précise des incidences sur la politique monétaire; cf. Banque Centrale Européenn, Report on Electronic Money, August 1998.

(29) Droit prélevé sur l'émission de monnaie fiduciaire et qui équivaut à la différence entre la valeur faciale des pièces et des billets et leur coût de fabrication.

techniques permettant des payements anonymes, comme il en existe déjà certaines.

Mais avec le développement de telles solutions, le risque pourrait se déplacer sur un autre terrain : celui d'une utilisation à des fins malhonnêtes comme le blanchiment d'argent provenant d'activités criminelles. Bien que ce danger paraisse évidemment plus circonstancié que le premier, le dilemme entre la nécessaire protection de la vie privée, comme élément essentiel de la dignité humaine et les contraintes imposées par la lutte contre les activités criminelles ne sera pas aisé à résoudre.

Sur un autre plan, l'avènement de nouvelles formes de « *monnaies électroniques* » lève également la question de la sanction des actes de falsification, voire de faux monnayage qui, en l'état actuel de nos ordres répressifs paraissent difficilement ressortir des délits existants (30).

Enfin, pour donner une ultime illustration des nombreuses interrogations que soulèvent les payements en ligne, il est permis de s'inquiéter du fait que la course vers des standards de sécurité de plus en plus élevés ne finisse par laisser pour compte ceux qui ne pourront plus s'en payer le luxe ou qui ne pourront y prétendre en raison notamment de leur jeune âge. Mais l'esprit de liberté régnant sur l'Internet tendra peut-être, à l'inverse, à fermer le fossé actuel entre les titulaires de cartes de payement ou de crédit et les personnes qui en demeurent privées. Des initiatives récentes (31) nourrissent cet espoir, tout en confrontant le juriste à de nouvelles difficultés...

(30) Communication de la Commission au Parlement européen, au Conseil, à la Banque Centrale européenne et au Comité économique et social, sur un cadre d'action pour la lutte contre la fraude et la contrefaçon des moyens de paiements autres que les espèces, juin 1998.

(31) DoughNet.com, RocketCash.com ou IcanBuy.com (récemment arrêté).