http://www.droit-technologie.org

présente :

DROIT DE LA CONCURRENCE ET SIGNATURE NUMÉRIQUE

QUELQUES RÉFLEXIONS À LA LUMIÈRE DE LA CONCENTRATION SWISSKEY SA

Michel JACCARD
Docteur en droit, LL.M. (Columbia),
Chargé de cours aux Universités de Fribourg et de Neuchâtel,
Admis au barreau de New York, avocat, Genève
jaccard@ttv.ch

28 novembre 2000

DROIT DE LA CONCURRENCE ET SIGNATURE NUMÉRIQUE

QUELQUES RÉFLEXIONS À LA LUMIÈRE DE LA CONCENTRATION SWISSKEY SA

(une version légèrement augmentée de ce texte a été publiée in: Revue suisse du droit de la propriété intellectuelle, de l'Information et de la Concurrence [Sic!], 1/1999, p. 17-25)

par

Michel JACCARD*

Au moment où la sécurité des transmissions sur Internet devient essentielle à l'essor du commerce électronique et alors que l'administration fédérale songe à réglementer juridiquement la signature numérique, Swisscom SA et Telekurs Holding SA ont formé avec les Chambres de commerce cantonales la première autorité de certification ("Cybernotaire") en Suisse. En raison de son actionnariat, cette concentration a dû être notifiée l'année dernière à la Commission de la concurrence, dont le secrétariat a dès lors entrepris un examen préliminaire au regard de l'article 10 LCart. Quelles options ont été prises pour la délimitation des marchés pertinents dans des domaines innovateurs et quelles cautèles ont été posées au regard des activités de la nouvelle société ?

I. Introduction

Le potentiel du commerce électronique ne sera pas pleinement réalisé avant la levée des incertitudes liées à l'identification des partenaires en ligne et à la confidentialité des transmissions, spécialement dans un environnement ouvert comme Internet. A cet égard, des systèmes de cryptographie asymétrique ou infrastructures à clé publique (*Public Key Infrastructure* - PKI) sont appelés à jouer un rôle crucial. Sans entrer dans les détails[1], de tels systèmes reposent sur l'utilisation d'une paire de clés mathématiquement correspondantes, l'une demeurant secrète et l'autre étant connue du destinataire des données. Avant son envoi, chaque message est compressé puis chiffré avec la clé secrète (ou privée) de l'expéditeur. Si le destinataire parvient à le déchiffrer à l'aide de la clé publique de l'expéditeur, il aura alors la quasi certitude mathématique que le message provient bien du titulaire de la clé secrète qui a permis le chiffrement et qu'il n'a pas été modifié lors de la transmission. Si l'expéditeur a non seulement signé les données de sa clé secrète, mais a également inclus dans l'algorithme de chiffrement la clé publique du destinataire, celui-ci aura en

---

* Docteur en droit, LL.M. (Columbia), Chargé de cours aux Universités de Fribourg et Neuchâtel, admis au barreau de New York, Avocat, TAVERNIER TSCHANZ, Genève (jaccard@ttv.ch).

1 Pour plus de précisions, voir M. JACCARD, Le rôle, le statut et la responsabilité de l'autorité de certification dans la transmission de données signées numériquement, *in:* Les contrats de distribution - Quelques aspects juridiques, Mélanges en l'honneur du Prof. F. DESSEMONTET à l'occasion de son 50ème anniversaire, CEDIDAC n° 38, Lausanne 1998, 403-428.

plus l'assurance qu'elles sont restées confidentielles, puisque sa propre clé secrète était nécessaire pour accéder aux données.

Pour assurer la fiabilité du système, un tiers doit impérativement garantir au destinataire l'identité de celui qui se prétend titulaire de la clé secrète utilisée pour la signature des données. Cette tâche essentielle est généralement accomplie par des autorités de certification (AC ou CA en anglais pour *Certification Authorities*). Outre des aspects de droit privé, en particulier en ce qui concerne la responsabilité[2], l'activité d'une autorité de certification soulève des questions de droit de la concurrence dans des marchés innovateurs qu'il n'est pas forcément aisé de délimiter, comme l'a démontré l'apparition sur le marché de la première autorité de certification suisse, Swisskey SA[3]. La société est contrôlée par Swisscom SA et Telekurs Holding SA. Y participe également l'association Digisigna, constituée des Chambres de commerce cantonales et de la Chambre de commerce de la Principauté du Liechtenstein.

Le cas de Swisskey SA présente un intérêt certain au plan juridique, puisqu'il a fait l'objet d'un examen préliminaire au regard de l'art. 10 de la loi fédérale sur les cartels et autres restrictions à la concurrence (LCart, RS 251). En l'espèce, la notification de la concentration était rendue obligatoire en raison des art. 9 al. 1 et 4 LCart, à savoir le dépassement des seuils minimaux et la position dominante de Swisscom SA (à l'époque Telecom PTT) constatée par la Commission de la concurrence dans l'affaire "Blue Window" moins d'un an auparavant[4].

Par décision du 6 avril 1998, la Commission de la concurrence, représentée par la Chambre des infrastructures, a estimé qu'un examen complémentaire approfondi de la concentration n'était pas nécessaire[5]. Avant de commenter brièvement cette décision, il faut d'abord rappeler en quoi consiste précisément l'activité d'une autorité de certification et quelles sont ses interactions possibles avec le droit de la concurrence.

II. Autorités de certification et droit de la concurrence

De manière générale, une autorité de certification procède vis-à-vis des personnes physiques ou des sociétés commerciales qui désirent faire authentifier leurs clés publiques (ci-après utilisateurs ou adhérents) selon les étapes suivantes :

- vérification de l'identité de l'adhérent lors de la demande de certificat (enregistrement);
- émission d'un certificat en format standardisé contenant au moins la clé publique de l'adhérent et des informations concernant son identité;
- signature du certificat par l'autorité de certification elle-même;
- mise à disposition du certificat ainsi authentifié sur un site en consultation libre, par exemple sur Internet;
- gestion du certificat (prise en compte des demandes de suspension et de révocation).

Indépendamment d'un quelconque système juridique, deux politiques sont généralement envisageables pour appréhender le phénomène de la certification publique dans une perspective de sécurisation du commerce électronique[6]: soit laisser libre cours au marché et privilégier l'auto-réglementation, en limitant l'intervention de l'Etat au respect de quelques principes fondamentaux, comme le fonctionnement d'une concurrence efficace; soit mettre en place un régime de surveillance, voire de concession pour l'octroi d'une licence à tout candidat à l'activité de

---

2 M. JACCARD (n. 1), 410-427.

3 <http://www.swisskey.com>.

4 RPW/DPC 2/1997, 161 ss.

5 RPW/DPC 2/1998, 252 ss.

6 Voir par exemple OCDE, *Dismantling the Barriers to Global Electronic Commerce* (disponible sur le site <http://www.oecd.org/dsti/sti/it/ec/prod/dismantl.htm>); OMC, Le commerce électronique et le rôle de l'OMC, Genève 1998; COMMUNICATION DE LA COMMISSION au Conseil, au Parlement européen, au Comité économique et social et au Comité des Régions, *La mondialisation et la société de l'information - La nécessité de renforcer la coordination internationale*, COM (98) 50 du 4 février 1998 (disponible sur le site <http://www.ispo.cec.be/eif/policy/>); INFORMATION INFRASTRUCTURE TASK FORCE, A framework for Global Electronic Commerce (disponible sur le site <http://www.iitf.nist.gov/eleccomm/ecomm.htm>).

certification, au vu des enjeux fondamentaux (atteinte à la liberté, risque d'anonymat favorisant l'activité terroriste ou criminelle, protection des données).

Ces approches coexistent aujourd'hui au plan mondial[7] et au sein des pays membres de l'Union européenne[8], où la récente proposition de directive sur un cadre commun pour les signatures électroniques préconise une reconnaissance mutuelle basée sur la transparence et l'absence de discrimination[9]. En Suisse, la position officielle consiste, semble-t-il, à privilégier une action législative pour la mise en place de la signature électronique à architecture PKI tout en reconnaissant l'importance du libre marché. Dans un rapport du Conseil fédéral de février 1998 consacré à la stratégie pour une société de l'information en Suisse[10], on peut lire en effet :

"La société de l'information se développe par le biais des initiatives de chacun et par l'effet de la libre concurrence. L'économie privée joue donc un rôle essentiel dans ce domaine; mais l'Etat veille à ce que sa configuration respecte les principes sociaux… Dans la société de l'information, le commerce électronique joue un rôle toujours plus grand. Il faut donc créer les conditions indispensables à l'utilisation fiable de cette application, harmonisées au niveau international, et respectant le principe d'égalité face au commerce traditionnel… Pour la mise en œuvre de ces mesures, le DFF et le DFEP sont chargés d'élaborer un concept et un plan d'action qui devront préciser notamment les objectifs, les mesures isolées devant être prises, les coûts, les partenariats, les procédures et le calendrier d'application. A titre de mesure immédiate, le DFJP et le DETEC sont chargés de l'introduction de la signature numérique pour laquelle ils devront concevoir un système de clé publique (Public Key Infrastructure) et élaborer les règles nécessaires".

A la suite de ce rapport, un groupe de travail interdépartemental ("DigSig") s'est formé sous la conduite de l'OFCOM et a mené une consultation auprès des milieux intéressés[11]. Sur la base des premiers documents disponibles[12], il semble que l'on s'oriente vers un système d'infrastructure à clé publique où l'Etat établirait le cadre de fonctionnement et la politique générale des autorités de certification par le biais d'un "organe de reconnaissance", qui pourrait être un office fédéral. L'accréditation auprès de cet organe demeurerait toutefois volontaire, pour assurer la compatibilité de la réglementation envisagée avec la proposition de directive communautaire et les projets d'uniformisation menés à l'échelle internationale. Le contrôle de l'Etat aurait en outre l'avantage de faciliter, à terme, la reconnaissance à l'étranger des autorités de certification accréditées en Suisse et d'améliorer la sécurité juridique par l'établissement de critères uniformes. En revanche, un tel schéma nécessiterait l'adoption de nouveaux textes législatifs sinon réglementaires, alors même que l'essor fantastique d'Internet est probablement lié à l'absence de sur-réglementation qui l'a caractérisé jusqu'à présent[13]. Par ailleurs, il serait regrettable de ne considérer qu'une infrastructure à clé publique, dans la mesure où d'autres technologies peut-être même plus fiables que la cryptographie asymétrique pourraient voir le jour dans un avenir proche[14]. Enfin et surtout, le risque de discrimination envers les autorités de certification non accréditées par l'Etat n'est pas négligeable.

---

7 COMMUNICATION DE LA COMMISSION au Conseil, au Parlement européen, au Comité économique et social et au Comité des Régions, *Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement*, COM (97) 503 du 8 octobre 1997, 18-20 (disponible sur le site <http://www.ispo.cec.be/eif/policy/>). A la suite d'une loi type sur le commerce électronique adoptée en 1996, la CNUDCI a d'ailleurs entrepris de nouveaux travaux d'uniformisation portant précisément sur la signature numérique et ses effes juridiques (voir en dernier lieu CNUDCI, A/CN.9/454 du 21 août 1998, disponible sur le site <http://www.un.or.at/uncitral/>).

8 COM (97) 503 du 8 octobre 1997 (n. 7), 10-11.

9 COMMUNICATION DE LA COMMISSION au Conseil, au Parlement européen, au Comité économique et social et au Comité des Régions, *Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques*, COM (98) 297 du 13 mai 1998, 13 (projet d'article 3) (disponible sur le site <http://www.ispo.cec.be/eif/policy/>).

10 Le texte du rapport est disponible sur le site de l'*Information Society Project Switzerland* (<http://www.isps.ch/>), qui contient également de nombreux liens et quantité d'informations sur l'évolution de la situation et de la stratégie des autorités politiques suisses.

11 Pour plus d'informations, voir <http://www.admin.ch/bakom/tc/DigSig/Index_f_DigSig.htm>.

12 GROUPE DE TRAVAIL INTERDÉPARTEMENTAL "DIGSIG", Signature numérique - Infrastructure à clé publique, Présentation du 24 novembre 1998 dans le cadre d'un séminaire organisé par l'OFCOM.

13 Ph. RUTTLEY, E.C. Competition Law in Cyberspace: An Overview of Recent Developments, [1998] ECLR 4, 203.

14 Dans le même sens, COM (97) 503 du 8 octobre 1997 (n. 7), 10.

C'est dans ce contexte d'analyse que le Secrétariat de la Commission de la concurrence devait procéder à l'examen préliminaire de la concentration Swisskey SA. La première étape consistait à délimiter quels marchés étaient pertinents, en application de l'article 11 al. 3 de l'Ordonnance sur le contrôle des concentrations d'entreprises du 17 juin 1996 (RS 251.4), qui distingue entre marché des produits et marché géographique à l'instar de la réglementation communautaire topique[15].

III. Délimitation des marchés pertinents

1. Du point de vue de l'activité (marché des produits)

Dans sa prise de position du 6 avril 1998, la Commission de la concurrence a retenu comme marché pertinent celui de la certification électronique, sans autre distinction (§18-§23). Dans le domaine des télécommunications, les marchés voisins de la transmission d'informations (§24-§26) et de l'accès à Internet (§27-§28) ont également été pris en compte, comme celui des cartes de crédit dans le domaine des moyens de paiement (§29-§31).

Or, la nature même de l'activité de tiers certificateur et la consultation du site Swisskey.com font apparaître que les prestations proposées sont (a) la fourniture d'un logiciel de génération de paires de clés, (b) l'enregistrement et l'émission de certificats et (c) le recensement et la consultation publique d'un registre des certificats et des clés publiques. Concrètement, l'utilisateur désireux de recourir aux services de Swisskey SA doit d'abord fournir la preuve de son identité, par une apparition physique à un guichet d'enregistrement, doté de pièces d'identité officielles et, le cas échéant, d'un extrait du registre du commerce légitimant son pouvoir. Pour l'instant, de tels guichets sont prévus auprès des Chambres de commerce cantonales[16]. Par ailleurs, Swisskey SA fournit à l'utilisateur un logiciel de génération de paires de clés cryptographiques (PayGuard). La clé publique ainsi générée est incorporée parmi les informations contenues dans le certificat lui-même, dans le format standard X.509 ou EDIFACT. Enfin, Swisskey SA elle-même garantit l'authenticité du certificat en le signant de sa propre clé secrète, avant de le mettre à disposition pour consultation dans un registre librement accessible.

A l'instar de la Commission européenne, il est dès lors possible de qualifier le marché concerné par l'activité de Swisskey SA d'*offre de services de certification publique*[17]. En outre, puisqu'elle fournit à l'utilisateur un logiciel qui permet de générer des paires de clés, Swisskey SA est également active sur le marché de l'*offre de cryptage (ou de chiffrement)*. La décision de la Commission de la concurrence ne reflète pas cette distinction, alors même qu'il s'agit d'un autre marché, qui consiste à fournir des outils de chiffrement capables d'assurer la confidentialité et l'intégrité de leurs transmissions en ligne[18]. Certaines autorités de certification, comme Swisskey SA, offrent directement les deux services[19].

Le marché de l'offre de services de certification publique et celui du chiffrement apparaissent eux-mêmes comme des *marchés connexes à celui du commerce électronique sécurisé*. Le lien entre la mise en place d'un système de signature numérique et l'essor du commerce électronique est aisé à saisir, si l'on rappelle que la cryptographie asymétrique est actuellement

---

15 COMMUNICATION DE LA COMMISSION sur la définition du marché en cause aux fins du droit communautaire de la concurrence, COM (97) 372/03 du 9 décembre 1997, JOCE n° C 372/5 du 9 décembre 1997 (également disponible sur le site de la DGIV, à l'adresse <http://europa.eu.int/comm/dg04/entente/fr/relevma.htm>).

16 <http://www.swisskey.ch/prod/pkg_html_show.p_show_page?iv_lang=2&iv_node=29> (site visité le 12 décembre 1998).

17 COM (97) 503 du 8 octobre 1997 (n. 7), 4.

18 Voir aussi COM (97) 503 du 8 octobre 1997 (n. 7), 2.

19 Par ailleurs et pour des raisons le plus souvent réglementaires (garantir au gouvernement l'accès aux données déchiffrées en tout temps), certaines autorités de certification, plus volontiers appelées alors tiers de confiance (*trusted third parties* ou *key escrow agents*), conservent également les clés privées de leurs clients sous écrou et pour leur compte.

la seule technique réellement viable qui soit susceptible de réduire les difficultés d'identification en ligne[20]. De façon surprenante, ce marché n'est pourtant pas mentionné dans la décision.

Dans le cas de Swisskey SA, autorité de certification publique, c'est le marché du commerce électronique sécurisé *en milieu ouvert* qui est visé, en ce sens qu'il lie principalement des partenaires occasionnels, par opposition aux transactions qui surviennent au sein d'un système fermé (intranets ou extranets)[21]. Dans ce dernier cas, les partenaires habituels se lient en général par des accords bilatéraux ou multilatéraux comportant des protocoles conventionnels de sécurité (conventions d'interchange)[22]. Quant aux types de partenaires occasionnels qui sont visés par les transactions à l'appui desquelles Swisskey SA se propose d'intervenir comme autorité de certification, il importe de relever que les utilisateurs visés sont autant les particuliers que les sociétés commerciales. Ainsi, les certificats peuvent être émis au nom d'une personne physique individuelle, d'une entité juridique, voire même d'un "processus" informatisé (*process*).

Puisqu'il est lié à celui du commerce électronique sécurisé, il faut peut-être encore mentionner le marché du *paiement électronique sécurisé en milieu ouvert*. En effet, l'achat d'un produit (même si la transaction se traduit encore par la livraison d'un objet physique) ou la demande d'un service en ligne se font le plus souvent par carte de crédit. Or, on constate aujourd'hui une réticence à fournir un numéro de carte et une date d'expiration en ligne, de peur de faire l'objet d'une fraude ou d'une interception illicite. Dès lors, le chiffrement de cette information couplé avec la clé publique du destinataire est un véritable gage de confidentialité et d'intégrité de la transmission, condition préalable nécessaire à l'essor des paiements en ligne. Le problème apparaît également si l'utilisateur ne fournit pas à chaque transaction une nouvelle information financière complète concernant sa carte de crédit, mais dispose de comptes auprès d'institutions "virtuelles", où l'identification intervient alors par le biais d'un mot de passe, qui doit lui aussi être protégé des regards indiscrets.

En revanche, le marché de *l'accès à Internet*, retenu par la Commission dans sa prise de position, ne me semble pas pertinent dans le cadre de l'examen préalable de la concentration Swisskey SA, dans la mesure où ni l'enregistrement d'un certificat ni la consultation du registre des clés n'est lié à une quelconque affiliation à un fournisseur particulier. De même, le marché de la *téléphonie*, également mentionné dans la prise de position (§32), apparaît plus proche du marché du chiffrement que de celui d'offre de services de certification publique. Il est vrai que le lien est étroit entre le commerce électronique et le coût des télécommunications et que les marchés respectifs sont certainement voisins sinon convergents[23]. Néanmoins, l'identification des interlocuteurs en téléphonie et la sécurisation de leurs communications ne passent pas par une autorité de certification. A cet égard, il faudrait peut-être réserver le développement prévisible de la téléphonie sur Internet, tout en précisant qu'il s'agirait alors vraisemblablement d'un marché distinct de celui de la téléphonie "traditionnelle", dans la mesure où Internet fonctionne sur le principe d'une facturation de la connexion toujours locale pour l'accès à un réseau global de communication. De toute manière, l'impact de la création de Swisskey SA sur un tel marché, qui serait certainement mondial du fait de la nature même d'Internet, est tout à fait négligeable, même dans une perspective dynamique[24].

2. Du point de vue géographique

En l'espèce, la délimitation géographique des différents marchés considérés revêtait une importance considérable. Il est en effet peu probable que l'examen préalable entrepris par le Secrétariat de la Commission eût débouché sur une enquête approfondie si les marchés considérés s'étaient étendus au-delà des seuls territoires suisse et liechtensteinois[25].

---

20 COM (97) 503 du 8 octobre 1997 (n. 7), 12; M. JACCARD, *Securing copyright in transnational cyberspace: the case for contracting with potential infringers*, Columbia Journal of Transnational Law 1997, 619 ss, spéc. 621-628.

21 COM (97) 503 du 8 octobre 1997 (n. 7), 1-2. Il est également vrai que des réseaux fermés pourraient avoir besoin de services de signature numérique, pour déterminer par exemple les personnes autorisées à prendre certains types de décision.

22 M. JACCARD, *La conclusion de contrats par ordinateur - Aspects juridiques de l'échange de données informatisées (EDI)*, ASR 583, Berne 1996, 151-186.

23 COM (98) 50 du 4 février 1998 (n. 6), 2-6.

24 Voir également les §32-§33 de la décision.

25 Art. 10 al. 4 LCart; Message du Conseil fédéral du 23 novembre 1994, n° 144.3; P. DUCREY / J. DROLSHAMMER, Kommentar zum schweizerischen Kartellgesetz, 2ème livraison, Zurich 1997, n. 18 et n. 35-38 *ad* art.

a) Marché du chiffrement par logiciel

Pour ce qui est du service de chiffrement, le marché pertinent n'est certainement pas limité à la Suisse. En effet, l'offre de services de chiffrement par le biais de logiciel est conséquente, puisque l'on recensait déjà en 1997 quelque 400 sociétés américaines et environ 440 sociétés non américaines actives sur un marché en pleine expansion[26]. En fait et notamment puisque les logiciels peuvent être acquis directement sur le réseau Internet, l'étendue géographique du marché ne sera limitée que par des réglementations étatiques restrictives, par exemple l'interdiction d'exportation, ce qui n'est toutefois pas le cas de la Suisse[27].

b) Marché de la certification publique

La délimitation géographique du marché de la certification publique est délicate. En effet, l'activité concrète d'un certificateur comporte des aspects multiples, dont certains sont typiquement locaux et d'autres au contraire globaux[28]. Comme observation générale, il est clair que la nature même du commerce électronique, véritable colonne vertébrale qui fonde toute activité d'une autorité de certification, est foncièrement internationale[29]. Internet a d'ailleurs parfois été décrit comme un monde sans frontières, annihilant espace et temps[30]. Cette caractéristique ne va pas sans susciter des problèmes dans des domaines autres que la certification électronique et qui sont rattachés au principe de territorialité, comme le droit d'auteur[31] ou le régime fiscal[32]. En faveur du caractère transnational d'un système de certification publique, on peut également mentionner le fait que le registre est consultable depuis le monde entier[33].

Surtout, un autre argument plaide en faveur d'un marché régional, sinon mondial de la certification publique : la question de l'autocertification, la nécessité de certifications en cascade ou encore la certification croisée ("*cross certification*"). Autrement dit, qui va certifier que l'autorité de certification qui se porte garante de l'authenticité du certificat consulté est bien celle qu'elle prétend être, dans la mesure où son identification résulte uniquement de sa propre signature du certificat délivré ? Pour résoudre ce problème, il faut donc instaurer un système de certification

---

10 LCart; R. WATTER / U. LEHMANN, Die Kontrolle von Unternehmenszusammenschlüssen im neuen Kartellgesetz, AJP/PJA 1996, 868 et 872.

26 COM (97) 503 du 8 octobre 1997 (n. 7), 12.

27 Pour un état des lieux des restrictions applicables en Europe et dans le monde, consulter par exemple <http://www.iki.fi/avs/eu-crypto.html> (visité le 12 décembre 1998 mais régulièrement mis à jour).

28 Voir aussi COM (97) 503 du 8 octobre 1997 (n. 7), 4.

29 Dans le même sens, COM (97) 503 du 8 octobre 1997 (n. 7), 11. Voir aussi Ph. RUTTLEY (n. 13), 195: "*Since access to the Internet is universal, it would be a rare occasion for an Internet transaction to be confined to a market that is less than global*".

30 A. SEGAL, *Dissemination of Digitized Music on the Internet: A Challenge to the Copyright Act*, Santa Clara Computer & High Technology Law Journal 1996, 99; D. JOHNSON / D. POST, *Laws and Borders - The Rise of Law in Cyberspace*, Stanford Law Review 1996, 1367; M. BURNSTEIN, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, Vanderbilt Journal of Transnational Law 1996, 102-114; D. MASSON, *Fixation on Fixation: Why Imposing Old Copyright Law on New Technology Will not Work*, Indiana Law Journal 1996, 1061 ss.

31 Voir par exemple J. GINSBURG, Extraterritoriality and Multiterritoriality in Copyright Infringement, Virginia Journal of International Law 1997, 587 ss; F. DESSEMONTET, Internet, le droit d'auteur et le droit international privé, RSJ 1996, 285 ss; M. JACCARD, Commerce électronique et droit d'auteur sur Internet, SZW/RSDA 2/1998, 57 ss.

32 COMMUNICATION DE LA COMMISSION au Conseil, au Parlement européen et au Comité économique et social, *Commerce électronique et fiscalité indirecte*, COM (98) 374 du 17 juin 1998 (disponible sur le site <http://www.ispo.cec.be/ecommerce/>).

33 A cet égard, il est significatif que Swisskey SA ait enregistré son nom de domaine Internet avec l'extension ".com", en plus du ".ch".

des autorités : soit une super-entité, soit un réseau d'autorités de certification doublé d'accords de reconnaissance mutuelle si des conditions minimales sont satisfaites[34].

D'un autre côté, Swisskey SA n'offre son service de certification publique *qu'aux entreprises avec siège en Suisse et aux personnes physiques résidant en Suisse*. Ainsi, la limite géographique aux services proposés est très clairement définie. Nous avons vu que l'enregistrement du certificat nécessite l'apparition physique de l'utilisateur. Le respect de cette procédure est un élément essentiel à la stratégie et au fonctionnement de Swisskey SA. Elle seule peut garantir une parfaite sécurité sur l'identité des personnes pour lesquelles Swisskey SA est disposée à émettre des certificats d'authenticité[35]. Comme la Commission de la concurrence le relève dans sa décision (§37-§38), cet élément est décisif pour la délimitation du marché, qui est dès lors certainement limité aux territoires suisse et liechtensteinois.

IV. Appréciation au regard des marchés retenus

1. Marché du chiffrement par logiciel

Ayant retenu un marché plus étendu que la Suisse pour le marché de l'offre de logiciels de chiffrement, les conditions matérielles de l'art. 10 al. 2 LCart ne sont pas remplies. Une réserve doit toutefois être formulée pour ce qui est des risques de transactions couplées (*tying arrangements*) du fait de la fourniture du logiciel PayGuard à tous les utilisateurs du service de certification publique de Swisskey SA[36].

2. Marché de la certification publique

Swisskey SA est la première autorité de certification suisse. Même dans une approche dynamique du marché, le statut particulier de Swisscom SA (opérateur historique, propriétaire d'installations, unique fournisseur de service universel de télécommunications et prestataire de services commerciaux dont "Blue Window") devait entraîner une vigilance particulière. Or, la Commission relève simplement dans sa prise de position que Swisskey SA devra faire face à des coûts supplémentaires que les entrants ultérieurs n'auraient pas à supporter (§59). Il est intéressant de remarquer que l'OFCOM, dans son appréciation du Livre vert européen sur la convergence du 3 décembre 1997, semble favoriser une approche plus stricte[37].

Il est par ailleurs évident que le marché de la certification publique est un marché où la confiance des utilisateurs est cruciale, puisqu'il s'agit de sécuriser les transactions électroniques sur un réseau comme Internet (*cf.* §56). A cet égard, Swisscom SA et Telekurs Holding SA bénéficient d'une légitimité qui renforce leur position[38] et Swisskey SA jouit sans conteste du fait de ses actionnaires d'une position privilégiée pour ce qui est de l'enregistrement des utilisateurs de services de certification publique. De plus, même s'il est vrai que les barrières ne sont pas techniques (§55), une assise financière conséquente sera nécessaire aux nouveaux entrants (promotion, investissements techniques, accords

---

34 Solution préconisée par l'Union Européenne, en particulier dans la proposition de directive sur un cadre juridique commun pour les signatures électroniques (voir COM (97) 503 du 8 octobre 1997 (n. 7), 18-19 et COM (98) 297 du 13 mai 1998 (n. 9), 6).

35 D'autres systèmes ne sont pas aussi sûrs. La société américaine Verisign, Inc. par exemple ne procède à aucune autre vérification pour ses *Class 1 digital IDs* que celle de la validité de l'adresse *email* du requérant (<http://www.verisign.com>).

36 Voir également le §63 de la décision.

37 Position de l'OFCOM sur le Livre vert sur la convergence des secteurs de télécommunications, des médias et des technologies de l'information, et les implications pour la réglementation, du 3 décembre 1997 [COM (97) 623], Avril 1998 (disponible sur le site <http://www.admin.ch/bakom>), Réponse (A) à Question 4: "Les entreprises qui occupent une position dominante sur le marché des infrastructures tout en produisant du contenu doivent être considérées sous un angle très critique, dans l'optique de l'économie et de la société. C'est spécialement à l'égard de celles-ci que la concurrence doit obéir à des règles strictes et claires."

38 Un argument semblable a déjà été mentionné dans l'affaire "Blue Window", *cf.* RPW/DPC 1997/2, 168, n° 44.

internationaux pour la certification croisée)[39]. De plus, n'oublions pas que le groupe de travail interdépartemental "DigSig" semble privilégier un système d'accréditation des autorités de certification, certes volontaire, mais qui aurait certainement pour effet d'ériger des obstacles réglementaires à l'accès au marché[40].

En outre, il existe un risque de voir Swisskey SA dominer le marché du simple fait de l'encouragement de ses actionnaires, dont indirectement les banques, à recourir aux services de Swisskey SA dans leurs nombreuses relations avec leur clientèle et d'exiger le même comportement de leurs partenaires commerciaux. Ce risque est peut-être encore plus concret pour les moyens de paiement électroniques, qui accompagnent pour ainsi dire chaque transaction commerciale sur un réseau ouvert. A nouveau, les utilisateurs de carte de crédit pourraient être incités à recourir au service de Swisskey SA pour continuer à entretenir des relations commerciales avec leur banque ou des institutions émettrices de cartes de crédit. Le raisonnement vaut à plus forte raison pour tous les commerces munis de systèmes à cartes de crédit, y compris les grands distributeurs.

Ainsi, la concentration Swisskey SA faisait apparaître des risques de création d'une position dominante sur un marché innovateur, que l'on peut tenter de résumer comme suit :

- Au niveau de *l'utilisation des services de certification*, risque de discrimination pour ce qui est de l'accès aux points de contact usuels avec la clientèle privée des actionnaires de Swisskey SA lors de la vérification de l'identité des futurs titulaires de certificats (§61).
- Au niveau du *commerce électronique sécurisé*, risque d'incitation à recourir aux services de Swisskey SA pour tous les partenaires commerciaux en contact avec ses actionnaires, à savoir principalement les usagers de la poste (malgré la séparation entre La Poste et Swisscom SA) et les clients bancaires (activités de télébanking), sans oublier les abonnés du service Blue Window de Swisscom SA.
- Au niveau du *paiement électronique sécurisé*, risque similaire d'incitation et de discrimination abusive pour la clientèle disposant de cartes de crédit, dont les institutions émettrices sont déjà actives au sein de Swisskey SA par le biais de son actionnaire Telekurs Holding SA.

Ces risques apparaissent particulièrement importants pour les utilisateurs individuels, qui, même s'ils sont des consommateurs actifs sur le réseau Internet, ne sont vraisemblablement pas enclins à souscrire à plusieurs services de certification (le problème se pose peut-être en termes différents pour les sociétés commerciales). Dès lors, un examen complémentaire de la concentration était certainement envisageable. Il aurait peut-être permis de savoir si les risques identifiés pouvaient être compensés par des effets positifs, comme par exemple le renforcement de la confiance dans un commerce électronique sécurisé en milieu ouvert, apte à entraîner une augmentation sensible du nombre et de l'importance économique des transactions en ligne. Mais la Commission a préféré mettre simplement en garde Swisskey SA contre toute tentative de discrimination quant aux prix pratiqués et aux possibilités d'accès aux points de contact avec la clientèle privée lors de la vérification de l'identité des futurs titulaires de certificats (§62).

Enfin, on peut relever que l'aspect innovateur de l'activité menée par Swisskey SA ne serait de toute manière pas de taille à masquer les obligations fondamentales découlant de l'art. 7 LCart[41]. Si besoin est, plusieurs litiges mettant aujourd'hui aux prises Microsoft Corp. et les autorités *antitrust* américaines nous rappellent également la nécessité d'être extrêmement vigilant quant aux risques qui découlent d'une position dominante et à la difficulté, une fois le marché dominé, d'obtenir un rééquilibrage par voie judiciaire[42].

V. Conclusion

Quelques semaines après l'entrée en vigueur de la nouvelle loi sur les télécommunications et quelques mois avant l'introduction en bourse de Swisscom SA, les autorités de concurrence ont dû entreprendre une étude préalable des effets d'une concentration envisagée dans un domaine essentiel à la sécurisation du commerce électronique. En ne bloquant pas l'opération, la Commission a manifestement pris la bonne décision, qui a pour conséquence immédiate

---

39 R. WATTER / U. LEHMANN (n. 25), 871. Voir aussi Ph. RUTTLEY (n. 13), 194.

40 Voir *supra*, n. 12.

41 Sur l'application éventuelle en droit suisse de la concurrence d'une analyse liée à l'innovation, voir B. BRECHBÜHL, Fusionskontrolle: Innovationsmarkt-Analyse und ihre Auswirkungen auf die Schweiz, SZW/RSDA 4/1998, 173 ss.

42 Pour un suivi des différentes procédures en cours, consulter par exemple <http://www.usdoj.gov/atr/cases/ms_index.htm>.

de positionner favorablement sur le nouveau marché les principaux acteurs déjà actifs dans le domaine des télécommunications et des paiements par carte de crédit. On peut toutefois regretter que les autorités de concurrence n'aient pas pleinement saisi l'occasion qui leur était offerte pour tenter de cerner précisément le phénomène de la sécurisation du commerce électronique et son impact sous l'angle du droit de la concurrence.

A cet égard, une analyse plus poussée aurait certainement permis de mieux définir les marchés concernés, d'envisager plus distinctement le comportement des utilisateurs futurs des services proposés et de mettre en lumière l'existence de barrières à l'entrée des marchés retenus. Le statut particulier de Swisscom SA, opérateur historique, propriétaire d'infrastructures et prestataire de services commerciaux, a peut-être été également négligé, alors même que les discussions intervenant au plan communautaire dans le domaine de la convergence, dont l'OFCOM s'est fait l'écho en Suisse, soulignent les risques spécifiques d'abus. Il reste que la Commission a insisté avec raison sur la nécessité de prévenir toute forme de discrimination. Espérons qu'elle n'hésitera pas, le cas échéant, à ouvrir une nouvelle enquête.