



**Le défi de l'identification
des consommateurs
dans le cadre des
nouveaux mécanismes
de paiement électronique**

Réalisé par Jacques St-Amant
et présenté au
Commissariat à la vie privée du Canada

Août 2006

OPTION CONSOMMATEURS

MISSION

Option consommateurs est une association sans but lucratif qui a pour mission de défendre les droits fondamentaux des citoyens-consommateurs tels qu'énoncés par les Nations unies en matière de protection des consommateurs et de veiller à ce qu'ils soient reconnus et respectés.

HISTORIQUE

L'association existe depuis 1983. En 1999, elle a regroupé ses activités avec l'Association des consommateurs du Québec (ACQ) qui existait depuis plus de 50 ans et accomplissait la même mission qu'Option consommateurs.

PRINCIPALES ACTIVITÉS

Option consommateurs compte sur une équipe d'une vingtaine d'employés qui oeuvrent au sein de quatre services : le Service budgétaire, le Service juridique, le Service d'agence de presse et le Service de recherche et de représentation. Au cours des ans, Option consommateurs a notamment développé une expertise dans les domaines des services financiers, de la santé et de l'agroalimentaire, de l'énergie, du voyage, de l'accès à la justice, des pratiques commerciales, de l'endettement et de la protection de la vie privée. Chaque année, nous rejoignons entre 7000 et 10 000 de consommateurs directement, nous réalisons de nombreuses entrevues dans les médias, nous siégeons à plusieurs comités de travail et conseils d'administration, nous réalisons des projets d'intervention d'envergure avec d'importants partenaires, nous produisons notamment des rapports de recherche, des mémoires, des guides d'achat dont le guide *Jouets* annuel du magazine *Protégez-Vous*.

MEMBERSHIP

Pour faire changer les choses, les actions d'Option consommateurs sont multiples : recherches, recours collectifs et pressions auprès des instances gouvernementales et des entreprises. Vous pouvez nous aider à en faire plus pour vous en devenant membre d'Option consommateurs : www.option-consommateurs.org

REMERCIEMENTS

Option consommateurs remercie le Commissariat à la vie privée du Canada pour son soutien financier à la réalisation de cette recherche.

La reproduction d'extraits limités du texte de ce rapport est permise, à condition d'en mentionner la source. Sa reproduction ou toute allusion à son contenu à des fins publicitaires ou lucratives sont toutefois strictement interdites.

Option consommateurs
2120, rue Sherbrooke est, bureau. 604
Montréal, Québec,
H2K 1C3

Téléphone : (514) 598-7288
Télécopieur : (514) 598-8511
Courriel: info@option-consommateurs.org

RESUME

L'évolution des pratiques en matière financière, et notamment en ce qui a trait aux paiements, change toutefois la donne. Ce phénomène se double évidemment des révolutions télématique et numérique. En matière bancaire notamment, de nouvelles techniques d'authentification des personnes par le recours à leurs caractéristiques biométriques deviennent par conséquent le sujet de réflexions et, parfois, de projets.

De telles initiatives comportent évidemment des avantages. Dans la mesure où elles fonctionnent, elles réduisent certains des risques associés à divers types d'opérations bancaires, au bénéfice des institutions financières comme de leurs clients. Mais fonctionnent-elles toujours si bien? Où en sommes-nous en matière d'identification des consommateurs lors de paiements électroniques? Entre autres et dans une dimension prospective, quels sont les inconvénients ou les dangers qui peuvent découler du recours aux identifiants biométriques dans le domaine bancaire au Canada?

Voilà les questions qu'il s'agit ici d'examiner, sous l'angle particulier de l'impact sur la protection des renseignements personnels relatifs aux clients des institutions financières. Il faudra évidemment poser d'abord le contexte d'ensemble et examiner tant l'évolution actuellement très rapide des modes de paiement que celle des modes d'identification ou d'authentification.

Il importe d'autre part de circonscrire notre champ d'intérêt. Nous nous intéressons au premier chef à la problématique de l'authentification dans le cadre des relations entre banquiers et consommateurs se livrant à des opérations de paiement. Si on abordera à l'occasion des processus d'authentification utilisés dans d'autres contextes, ce ne sera qu'à titre accessoire et illustratif.

Les questions reliées à l'authentification sont étroitement liées à certaines de celles touchant la sécurité; elles en sont toutefois distinctes et nous ne ferons ici qu'effleurer la problématique de la sécurité des opérations de paiement, beaucoup plus vaste et à bien des égards tout à fait différente.

Option consommateurs	i
Remerciements	II
Résumé	III
I- La mise en contexte	1
A- La problématique	1
B- Des hypothèses et une méthode	1
C- Une terminologie	2
D- La gestion de risque	6
II- L'identité et l'authentification	8
A- Reconnaître	8
B- Comment authentifier?	10
1- la présentation de l'éventail	10
2- les caractéristiques recherchées	12
III- L'authentification et le banquier	13
A- L'obligation d'authentifier	13
B- Les modalités de l'authentification	14
1- le dépôt et le paiement	15
2- l'opération de crédit	17
C- L'évolution des marchés	19
D- L'allocation des risques	22
E- Les méthodes d'authentification	24
1- la signature	24
2- le modèle de la clé	26
3- le modèle du mot de passe	27
4- le modèle de l'apparence	29
5- l'identification à deux facteurs	30
F- L'état des choses	33

IV- L'authentification biométrique: un survol	33
A- Quelques illustrations	33
B- Des difficultés d'ordre général	34
B- Une recension partielle	38
1- les identifiants biométriques morphologiques	39
a) la dactyloscopie	39
i) des empreintes confuses?	39
ii) des défis pratiques	42
iii) des résultats insatisfaisants	45
b) l'observation de l'iris	47
c) la comparaison faciale	51
2- les autres identifiants biométriques	52
V- La question de l'architecture	53
A- Un problème systémique	53
B- Trouver l'équilibre	55
C- Biométrie et autres solutions	57
D- Que faire?	59

I- La mise en contexte

A- La problématique

Dans le *Marchand de Venise*, le Shylock de Shakespeare réclamait déjà en paiement *a pound of flesh*¹: le lien entre la dimension organique de ceux qui paient et leurs financiers ne date pas d'hier... Bien avant cela, la signature a joué un rôle déterminant dans le commerce ou les affaires publiques. Mais surtout et d'âge immémorial, les gens se reconnaissent physiquement et cela tient à leurs traits, à leur voix, à leur posture... Simplement et à la manière de M. Jourdain, on fait depuis toujours de la biométrie sans le savoir.

L'évolution des pratiques en matière financière, et notamment en ce qui a trait aux paiements, change toutefois la donne. Ce phénomène se double évidemment des révolutions télématique et numérique. En matière bancaire notamment, de nouvelles techniques d'authentification des personnes par le recours à leurs caractéristiques biométriques deviennent par conséquent le sujet de réflexions et, parfois, de projets.

De telles initiatives comportent évidemment des avantages. Dans la mesure où elles fonctionnent, elles réduisent certains des risques associés à divers types d'opérations bancaires, au bénéfice des institutions financières comme de leurs clients. Mais fonctionnent-elles toujours si bien? Où en sommes-nous en matière d'identification des consommateurs lors de paiements électroniques? Entre autres et dans une dimension prospective, quels sont les inconvénients ou les dangers qui peuvent découler du recours aux identifiants biométriques dans le domaine bancaire au Canada?

Voilà les questions qu'il s'agit ici d'examiner, sous l'angle particulier de l'impact sur la protection des renseignements personnels relatifs aux clients des institutions financières. Il faudra évidemment poser d'abord le contexte d'ensemble et examiner tant l'évolution actuellement très rapide des modes de paiement que celle des modes d'identification ou d'authentification.

B- Des hypothèses et une méthode

On esquissera les premiers éléments de cette analyse dans les prochaines pages. La réflexion sera notamment guidée par deux (2) hypothèses:

¹ On ignore si cette comédie dans laquelle Shakespeare a créé un personnage devenu légendaire a été écrite en 1594 ou 1596.

- (1) les modes d'authentification électronique présentement déployés dans le marché ou susceptibles de l'être en matière de paiement comportent des lacunes souvent méconnues mais appréciables au plan de l'efficacité ou de l'efficience;
- (2) certains nouveaux modes d'identification envisagés dans ce domaine, dont les identifiants biométriques, comportent également des lacunes au plan de la sécurité et ne sont pas non plus bien adaptés aux besoins de l'ensemble des consommateurs.

Au plan méthodologique, on a ici fait appel à deux (2) types de ressources complémentaires. On a d'une part recensé une partie de la documentation écrite relative à ces questions, dans les sources spécialisées comme dans la presse. On a d'autre part effectué des vérifications pratiques sur le terrain et communiqué avec divers acteurs afin d'établir certains faits importants.

Il importe d'autre part de circonscrire notre champ d'intérêt. Nous nous intéressons au premier chef à la problématique de l'authentification dans le cadre des relations entre banquiers et consommateurs se livrant à des opérations de paiement. Si on abordera à l'occasion des processus d'authentification utilisés dans d'autres contextes, ce ne sera qu'à titre accessoire et illustratif.

Les questions reliées à l'authentification sont étroitement liées à certaines de celles touchant la sécurité; elles en sont toutefois distinctes et nous ne ferons ici qu'effleurer la problématique de la sécurité des opérations de paiement, beaucoup plus vaste et à bien des égards tout à fait différente.

C- Une terminologie

À problèmes nouveaux, vocabulaire renouvelé. Il convient en effet de s'entendre sur le sens qu'on donnera ici à divers vocables. Certains ne prêtent guère à controverse. Dans d'autres cas, on assiste encore ici et là à des querelles de clocher quant à l'acception exacte des termes de l'art. On ne tentera pas ici de trancher entre ces écoles et on retiendra des définitions qui, à la fois, conviennent à nos fins et sont assez largement acceptées.

D'abord, on entend par «clients» ou «consommateurs» des personnes physiques agissant à des fins autres que d'entreprise.

On entend par «banques» ou «banquiers» les institutions financières qui font «commerce de banque». Notamment si elles acceptent des dépôts, traitent des ordres de

paiement et consentent des prêts. On inclut donc évidemment dans cette catégorie les banques canadiennes elles-mêmes, au sens technique du terme, mais aussi les coopératives de services financiers, les caisses d'épargne et de crédit, les sociétés de fiducie et, plus globalement, toute institution financière membre de l'Association canadienne des paiements qui réalise des opérations de banque avec des consommateurs².

On entend d'autre part par «commerçant», une personne ou une entité exploitant une entreprise et, dans le contexte qui nous intéresse, qui accepte des paiements sous forme électronique, et par exemple par carte de débit, par carte de crédit, par carte prépayée ou par l'Internet.

Pour simplifier, on accordera ici en général une acception assez large à la notion de «personne» afin d'y inclure les personnes physiques, les personnes morales et les autres entités exerçant une activité et dotées d'un nom ou d'attributs qui permettent de les distinguer. Toutes les formes d'entreprises, notamment, s'y trouvent par conséquent subsumées. Au besoin, on distinguera la «personne physique».

La notion d'identité pose à la réflexion des difficultés plus considérables qu'on ne pourrait le croire au premier abord – et c'est après tout le thème de cette recherche. Bien sûr, elle évoque d'abord le nom d'une personne, ou des renseignements qu'on associe fréquemment au nom, comme l'adresse par exemple: on pourrait parler génériquement d'«identification» de la personne. Mais ce qui fait l'identité d'une personne physique, c'est aussi ce qu'elle sait ou ce qu'elle est morphologiquement, entre autres composantes: le nom ne constitue somme toute qu'une étiquette associée à un être complexe. L'identité inclut aussi des éléments comme l'appartenance ethno-culturelle ou les habitudes³, y compris les habitudes de consommation: la personne ne se reconnaît pas comme étant simplement un nom ou un numéro, elle est bien davantage.

L'identité renvoie donc à l'individu particulier, mais aussi à une kyrielle de caractéristiques qui constituent des facteurs d'appartenance. On ne s'étonne pas dans ce contexte que la définition que donne de la notion de «données à caractère personnel» la

² Nous n'ignorons certes pas que d'autres types d'entreprises occupent de plus en plus de place dans le marché des paiements, comme par exemple la société PayPal, associée à eBay; pour nos fins, elles ne constituent toutefois pas (du moins pour l'instant) un phénomène qui requerrait qu'on les distingue des institutions financières et, dans le marché canadien au moins, on peut pour l'essentiel s'en tenir à ces dernières.

³ Le vocable «habitude» dérive après tout de racines latines désignant la «manière d'être».

directive européenne relative au traitement de telles données⁴ renvoie explicitement à l'«identité physique, physiologique, psychique, économique, culturelle ou sociale» de la personne⁵.

Sauf lorsque le contexte s'y oppose, on retiendra ici une acception étendue de la notion d'«identité», et on utilisera pour évoquer certains attributs rattachés à un individu précis (comme le nom) la notion d'«identité particulière». En définitive, l'identité réelle d'une personne procède d'une somme d'identifiants. Et une personne peut se trouver identifiée par un quelconque sous-ensemble de ces attributs, d'où il résulte qu'une personne peut détenir plusieurs «identités», selon la perspective selon laquelle on l'envisage. Bien sûr, ce sont ici ses diverses identités particulières biométriques qui retiendront principalement notre attention.

La notion d'«identification» renvoie aux processus et aux techniques utilisés afin d'établir l'identité d'un consommateur ou d'une entreprise, et notamment son identité particulière. Identifier une personne, c'est lui rattacher certaines informations⁶, certains attributs. Quand on procède à une identification, on cherche au fond à répondre à la question: «Qui êtes-vous?»⁷

Celle d'«autorisation» englobe les processus et les techniques utilisés afin d'établir qu'une personne se trouve effectivement titulaire des droits ou des privilèges qu'elle entend exercer⁸, ou qu'un attribut peut bien être rattaché à quelque chose.

L'«authentification» vise à prouver la véracité d'un énoncé en matière d'identification ou d'autorisation⁹. C'est une chose que d'affirmer être le premier

⁴ Union européenne. *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. J.O. no 281 du 23/11/95 pp. 0031-0050. (Ci-après également la «Directive européenne»).

⁵ *Ibid.*, al. 2 a).

⁶ Clarke, Roger. *Human Identification in Information Systems: Management Challenges and Public Policy Issues*. Canberra, Xamax Consultancy Pty Ltd., 1994. On trouvera ce document au [www.anu.edu.au/people/Roger.Clarke/DV/Humain ID.html](http://www.anu.edu.au/people/Roger.Clarke/DV/Humain%20ID.html). Dans cette mesure, l'identification constitue une quelque sorte une opération commutative, réversible: on rattache des informations à une personne, et donc on rattache une personne à des informations.

⁷ Schneir, Bruce. *Beyond Fear*. New York, Copernicus Books, 2003. 295 p. Pp. 182, 184-186. Bruce Schneir est un expert reconnu en matière de sécurité.

⁸ *Ibid.*, pp. 183-184. Ces deux définitions sont également inspirées de la terminologie retenue par la Banque des règlements internationaux: Basel Committee on Banking Supervision. *Risk Management Principles for Electronic Banking*. Bâle, Banque des règlements internationaux, juillet 2003. P. 13. 29 p.

⁹ Cette notion d'authentification est plus large que celle retenue dans l'«ébauche pour consultation» des Principes d'identification électronique élaborée par la Direction générale du commerce

ministre du Canada: c'en est une autre que d'en avoir les traits ou la signature et c'est le constat de la présence ou de l'absence de caractéristiques particulières qui permet de déterminer si l'individu qui fait cette assertion est bien celui qu'il dit être.

Pour sa part, le concept d'«attribut» désigne un élément informationnel concernant l'identité, un droit, un privilège ou une autre caractéristique rattachée à une personne, à un objet ou à une autre information¹⁰.

Il convient par ailleurs de souligner un aspect de la problématique qui découle de deux (2) de ces définitions – et non pas tant en raison de leur libellé que parce qu'il s'agit bien de concepts différents: l'identification et l'autorisation ne se confondent pas conceptuellement (même si elles semblent souvent le faire en pratique), et soulèvent chacune leur part de difficulté.

Quand on identifie, on donne une identité. Souvent (mais pas toujours), on individualise une personne¹¹. On la distingue, et parfois on la nomme (ou on la numérote...), pour certaines fins du moins. La difficulté primordiale vient bien sûr de ce qu'on peut se tromper: on peut attribuer à une personne une identité à laquelle elle n'a pas droit. Ou, inversement, on peut refuser une identité à une personne qui y a droit, conclure qu'elle n'est pas qui elle est pourtant.

L'identification constitue donc un processus délicat, mais qui n'a généralement pas besoin d'être répété au sein d'un système donné, et il se situe habituellement assez près du début de la relation entre une personne et un système. On peut en donner pour exemples la confection de l'acte de naissance qui, sur la foi du témoignage des parents et du médecin, atteste du nom, de la filiation et du moment de la naissance, ou l'émission par un employeur d'un identifiant à un nouveau salarié sur la foi du témoignage d'un cadre qui confirme que cette personne peut désormais entrer dans le lieu de travail. La captation d'une caractéristique biométrique d'un consommateur au moment de l'ouverture de son compte bancaire constituerait également une opération d'identification.

électronique d'Industrie Canada sous les auspices du Groupe de travail sur les principes d'authentification, qui renvoie quant à elle davantage à l'autorisation. Quant à ce document, Industrie Canada – Direction générale du commerce électronique. *Principes d'authentification électronique - Ébauche pour consultation*. Ottawa, Industrie Canada, 23 juin 2003. P. 4. (Ci-après également l'«Ébauche»). 20 p.

¹⁰ Brands, Stefan. *Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy*. Cambridge (Mass.), The MIT Press, 2000. 314 p. P. 9. Le Dr Brands emprunte par ailleurs ce concept à la terminologie utilisée en normalisation internationale.

¹¹ On peut en effet «identifier» une personne comme constituant un client potentiel pour un bien ou un service quelconque, sans détenir pour autant de renseignements précis sur son identité particulière. C'est alors l'appartenance à un groupe qui sera établie.

L'autorisation vise notamment à vérifier qu'une personne donnée a déjà été identifiée, et donc qu'elle détient bien certains droits ou doit faire face à certaines obligations. Pour nos fins, elle comporte le plus souvent deux (2) éléments: la personne doit présenter un identifiant qui lui soit légitimement associé, et on doit en contrôler la validité. L'autorisation peut cependant viser aussi l'établissement de la qualité d'autres attributs qu'un identifiant particulier, comme la validité d'un instrument de paiement électronique anonyme, par exemple¹².

L'autorisation a donc dans bien des cas vocation à se répéter, et parfois fréquemment, tout au long de la relation entre une personne et un système. Le salarié présentant sa carte pour entrer au travail, le consommateur composant son numéro d'identification personnel à un guichet automatique, ou celui qui y fournirait la caractéristique biométrique captée lors de l'ouverture de compte, passent par un processus d'autorisation qui vise à confirmer qu'ils peuvent accéder à l'usine ou qu'un paiement peut être effectué.

Le succès d'un mécanisme d'autorisation requiert notamment qu'on évite deux (2) écueils: la contrefaçon d'un identifiant ou l'usage non autorisé d'un identifiant valide. Pour la partie qui cherche à reconnaître quelqu'un ou quelque chose, l'objectif fondamental ne varie toutefois pas, qu'il s'agisse d'identification ou d'autorisation: il s'agit de vérifier une donnée servant à opérer un choix. On voudra donc être relativement certain de l'authenticité de cette donnée, pour éviter les erreurs et contrôler les risques. Pour celui qui veut être autorisé, il s'agit simplement qu'il soit reconnu, encore qu'il sache bien lui-même qui il est. Déjà, on perçoit les défis qui attendent identificateur et identifié. Avant de les analyser, il faut toutefois poser plus précisément un certain nombre d'éléments qui pourront guider la réflexion.

D- La gestion de risque

Dans une certaine mesure, la problématique qui nous intéresse. peut être ramenée à une question de gestion de risque – ou, plus précisément, à quelques questions de cette nature. Il existe en effet plusieurs types de risque, dont la nomenclature varie selon les sources, mais dont certains sont particulièrement pertinents pour nos fins¹³: on pense

¹² par analogie et dans le monde non-virtuel, la vérification d'un billet de banque afin de s'assurer qu'il n'est pas contrefait constitue un processus d'autorisation au sens où on l'entend ici.

¹³ La gestion de risque constitue un domaine d'étude en soi, dans le détail duquel on n'entrera pas ici. On retiendra seulement, et sommairement, certaines catégories de risques bien identifiées dans le

notamment au risque juridique, au risque d'exploitation, au risque de liquidité, au risque de crédit et au risque réputationnel.

Le risque juridique comporte de nombreux volets. Il s'agit d'abord pour une personne de se conformer aux règles (dont la législation) qui s'appliquent à elle – et qui peuvent changer. La conformité de cette personne à ses obligations contractuelles s'apparente aussi à ce premier aspect du risque juridique. Elle peut aussi encourir un risque juridique dans la mesure où ses cocontractants ou d'autres acteurs ne se conforment pas à leurs obligations légales à son endroit. En somme, tout ce qui déroge à la règle de droit relève du risque juridique; l'incertitude du droit dans un domaine donné accroît évidemment le risque, puisqu'on peut ne constater qu'*a posteriori* qu'on a agi sans droit, et elle rend aussi ce risque moins aisément quantifiable.

Quant au risque d'exploitation, il a trait à la possibilité de subir des pertes en raison de l'inadéquation ou de l'échec des processus, de la technologie ou de facteurs humains, par exemple. C'est l'erreur administrative, mais c'est aussi par exemple l'insuffisance des mesures de sécurité qui facilite un vol ou la panne qui rend les systèmes inutilisables pendant quelques heures.

Le risque de liquidité envisage principalement pour nos fins les situations où une institution financière ne dispose plus des liquidités requises pour faire face à ses obligations au fur et à mesure de leur échéance. Dans une acception plus restreinte, on y renverra ici pour englober les situations à une institution financière a erronément réduit son actif en remettant à une personne des sommes auxquelles cette dernière n'avait pas droit; l'institution voudra alors répéter ces montants, mais ne peut être assurée d'y parvenir, et peut donc subir une perte monétaire.

Le risque de crédit constitue une préoccupation constante du banquier. Il s'agit du risque qu'il encourt en raison de l'incapacité d'un débiteur de remplir ses obligations de remboursement. La notion de «risque réputationnel», enfin, parle d'elle-même: si une personne, et notamment un banquier, commet des erreurs sérieuses, la chose peut se savoir et entamer la confiance de la population envers l'institution, avec les effets commerciaux, financiers et juridiques que cela peut entraîner.

Débiteur et créancier courent dans certains cas un risque juridique s'ils n'ont pas identifié adéquatement leur cocontractant ou authentifié la qualité du paiement qu'ils ont

secteur financier canadien. Le lecteur intéressé aussi pourra consulter les quelques pages consacrées à cette question dans St Amant, Jacques. *Le cadre juridique des paiements électroniques au Canada: quand Fortune se fait virtuelle*. Montréal, Option consommateurs, 2002. 303 p. Pp. 278-283.

cru recevoir, par exemple. La nature précise et l'ampleur de ce risque varient toutefois selon les circonstances. Le banquier peut d'autre part et manifestement encourir des pertes en raison de risques d'exploitation (au plan de la sécurité, par exemple), mais le consommateur peut également en être victime à divers égards: il sera agacé par un site inaccessible ou peu convivial, mais il pourra voir ses identifiants volés après qu'il les ait confiés à l'exploitant d'un site mal défendu contre les attaques pirates.

II- L'identité et l'authentification

A- Reconnaître

Αυτογραφειν: littéralement, «écrire soi». L'autographe fait donc un peu office d'archétype de la trace persistante qui vise à identifier une personne ou à contrôler son identité. Le droit, notamment dans le cadre du contrat, y a souvent recours. Mais l'étranger peut inventer ou contrefaire une identité ainsi que la signature y associée. De toute manière, le contrôle à distance de la conformité de l'autographe traditionnel pose sa part de problèmes.

Le sujet pensant sait bien qui il est (sauf aberration cognitive). Ses proches, qui l'ont connu dès le berceau, le reconnaissent également, à certains signes d'ordre morphologique ou sociologique notamment¹⁴. Au sein de son clan, puis plus tard de son village, l'individu est donc en principe identifié: la communauté sait «naturellement» qui sont les siens et quel rôle ils y jouent. L'inconnu, c'est l'étranger. Ou celui qui est devenu tel. Mais il arrive qu'on se trompe.

La triste histoire de l'intrigant Martin Guerre l'illustre éloquemment¹⁵. Elle se déroule dans le bourg d'Artigat, au sud de la France¹⁶, dans la seconde moitié du seizième siècle. Martin, jeune marié, est malheureux au village. Il s'en enfuit pour aller à la guerre,

¹⁴ Et à défaut de reconnaître l'individu lui-même, on reconnaîtra par exemple au moins sa qualité de soldat à son uniforme.

¹⁵ Il s'agit d'une histoire vraie, attestée par des documents historiques. Elle a cependant donné lieu à une production littéraire et artistique importante, à commencer par la relation qu'en a publiée dès 1561 le juge rapporteur du procès en appel, Me Jean de Corat. Des cinéastes français en ont aussi tiré un film au début des années 1980, qui mettait en vedette Gérard Depardieu et Nathalie Baye. On trouvera à la fois le récit de ce film et une étude historique approfondie de l'affaire dans Davis, Natalie Z.; Carrière, Jean-Claude; Vigne, Daniel. *Le retour de Martin Guerre*. Paris, Robert Laffont, 1982. 269 p.

¹⁶ Artigat relevait alors administrativement du Languedoc, et se trouve maintenant dans le département d'Ariège.

tout comme un homme d'ailleurs qui l'a peut-être connu et qui lui ressemble, Arnaud du Tilh¹⁷. Martin est estropié au combat. Arnaud, lui, quitte l'armée et se rend à Artigat où il affirme être Martin et en prend le nom, le rôle au village et l'épouse. Ceux qui doutent clignent doucement des yeux pour la plupart¹⁸.

Tout va donc bien pour Arnaud jusqu'à ce qu'une querelle d'argent soulève les passions familiales: il est alors dénoncé pour usurpation d'identité, puis jugé¹⁹. Il paraît néanmoins en passe de triompher jusqu'à ce que le véritable Martin Guerre fasse lui-même irruption au procès et y soit par tous reconnu. Arnaud du Tilh est pendu à Artigat, et son corps brûlé, le 16 septembre 1560.

Voilà qui pose plutôt dramatiquement le problème qu'il s'agit de cerner. À quoi reconnaît-on une personne? Dans quelles circonstances importe-t-il de la reconnaître? Et, tout comme au seizième siècle, le choc des intérêts d'argent fournit fréquemment l'occasion de s'interroger à l'égard de l'identité d'un inconnu.

Or les méthodes traditionnelles qui permettaient de reconnaître une personne ne suffisent plus. Le village a grandi en effet: il devient planétaire. Les opérations commerciales se font à distance et par ordinateurs interposés: l'essor du commerce électronique change donc notablement la donne. On «rencontre» maintenant bien plus d'inconnus avec qui on veut traiter, tandis que les outils technologiques simplifient souvent la fraude. L'homme se trouve le plus souvent un étranger pour son semblable.

Il faut dès lors choisir: on ne fait pas de commerce électronique, et notamment d'opérations de paiement, ni d'opérations électronique à distance en général, avec les inconnus (et donc on en fait peu), on en fait même s'ils demeurent des inconnus (avec les risques concomitants), ou on se dote de moyens de reconnaître les inconnus, de les identifier, pour faire commerce avec eux, et il faut alors songer à consentir un effort considérable. Les méthodes appliquées doivent en effet être efficaces et efficaces,

¹⁷ Arnaud provenait d'un autre village; les données historiques ne permettent pas d'établir avec certitude dans quelle mesure Arnaud et Martin se sont connus. Il s'est écoulé 8 ans entre la fuite de Martin Guerre et l'arrivée d'Arnaud à Artigat.

¹⁸ Le procès permet de constater comment on a cherché à confirmer ou infirmer l'identité de «Martin Guerre»: d'abord, lui-même reconnaissait les villageois et connaissait nombre d'anecdotes propres à la vie de Martin Guerre, y compris certains détails de sa vie conjugale antérieure. Ensuite, il est reconnu physiquement à son apparence, y compris l'état de sa dentition ou la taille de ses pieds (selon le témoignage du cordonnier). Bref, on s'intéresse à ce que sait l'individu et à ce qu'il est physiquement: au fond, on n'a pas beaucoup progressé depuis 440 ans...

¹⁹ localement d'abord, à Toulouse ensuite.

puisqu'on doit pouvoir se fier à la vérification, sans que le processus soit indûment rebutant pour ceux qui identifient comme pour ceux qui s'identifient.

Or le défi de l'identification ou de l'authentification est complexe à de multiples égards. Il soulève, on le verra, des problèmes techniques importants. Mais, et on inclinera à croire «surtout», il touche à ce que la personne a de plus essentiel. Elle se sait multiple; le tiers veut reconnaître l'individu, et de la manière qui lui convient. Ce tiers veut choisir l'attribut identifiant, peut-être même le posséder²⁰, et y réduire l'individu comme cela lui convient. La personne s'en trouve méconnue, dépossédée, aliénée: l'identifiant imposé à une personne par un élément de la société devient plus important pour les autres que son identité globale.

Ces processus ont évolué organiquement, graduellement depuis un siècle ou deux, avec la fixation de la structure du nom individuel et la généralisation de la signature, puis de la photo à titre de preuves d'identité. Ils se précipitent maintenant, à la faveur de l'émergence de nouveaux moyens technologiques et de besoins commerciaux redéfinis, sans que les citoyens aient le sentiment d'avoir voix au chapitre et sans qu'on s'arrête outre mesure aux conséquences juridiques, sociologiques, psychologiques ou politiques de ces mutations de la perception et du rôle de l'identité.

B- Comment authentifier?

1- la présentation de l'éventail

On a pris depuis quelques années l'habitude de classer les méthodes d'identification ou d'authentification en trois (3) grandes catégories: on recourra à ce qu'une personne sait, à ce qu'elle détient ou à ce qu'elle est²¹. Donnons pour exemples respectifs le numéro d'identification personnelle, la carte magnétique et l'empreinte digitale. Il faut toutefois prendre aussi en compte une quatrième méthode, qui suscite un regain d'intérêt: on peut reconnaître une personne à ce que les autres en disent. Ce sera

²⁰ Tout comme les émetteurs de cartes de crédit entendent posséder le numéro qu'elles attribuent à la carte d'un détenteur ou comme les sociétés de télécommunication se disent propriétaires du numéro de téléphone qu'elles attribuent à un abonné: à ce dernier égard, l'alinéa 14 (1) des Modalités de service de Bell Canada précise par exemple que «[L]es abonnés n'ont aucun droit de propriété sur les numéros qui leur sont attribués»: Bell Canada. *Annuaire Montréal 2003*. Bell Actimédia Inc. slnd.

²¹ À titre d'exemple, Schneier, *op. cit.*, p. 186.

par exemple le cas d'un organisme d'accréditation qui atteste des caractéristiques de tel ou tel adhérent²².

Et il s'en développe une cinquième: on reconnaît également les gens à ce qu'ils font. Ou du moins, on croit pouvoir le faire. Et donc on confectionne des profils qu'on veut prédictifs. Encore là, on réduirait la personne à une trajectoire déterminable. Si elle fournit des approximations utilisables à l'échelle des communautés, l'analyse des comportements ne permet pas encore une identification fiable des individus et elle demeure tributaire d'autres modes d'authentification.

Malheureusement, toutes ces méthodes comportent des lacunes. L'objet qui fait office de sésame peut être volé. Le code, ou toute autre information qu'on veut propre à la personne²³, peut être usurpé parce qu'il y aura eu espionnage d'un tiers, négligence du détenteur ou, simplement, attaque massive par un fraudeur. Le recours à des caractéristiques physiques requiert l'usage d'une quincaillerie particulière, il peut s'avérer compliqué dans le cas de relations à distance, il n'est pas d'une fiabilité absolue et il risque d'être mal perçu par une partie au moins de la population²⁴.

Et, bien sûr, celui qui identifie détient des informations qui lui permettent de reconnaître son interlocuteur; dans bien des cas, il pourrait lui-même utiliser ces informations pour usurper des identités, ce qui pose un grave problème au plan de la sécurité²⁵.

Il importe aussi de noter que cette taxonomie des modes d'identification comporte des zones grises. Songeons par exemple au nom de la personne: on l'associe souvent à la catégorie de ce qu'«est» une personne, mais il s'agit aussi de quelque chose qu'elle sait²⁶.

²² Bien sûr, il faudra aussi authentifier cette attestation, en recourant à l'une ou l'autre de ces 4 grandes méthodes, ou à d'autres moyens – car cette typologie n'est pas exhaustive.

²³ On sait par exemple que plusieurs émetteurs de cartes de crédit utilisent, à titre d'identifiant supplémentaire, le patronyme de la mère du détenteur de la carte.

²⁴ À court terme, on imagine mal qu'on équipe tous les internautes d'un équipement permettant de capter leurs empreintes digitales, par exemple, et il est probable que le stigmate rattaché à la dactyloscopie parce qu'elle sert depuis des décennies à identifier les criminels joue contre le recours à une telle méthode. De toute manière, ces méthodes ne sont pas non plus absolument fiables. On y revient *infra*.

²⁵ Et si ce n'est pas l'entreprise elle-même, ce pourrait être par exemple un de ses employés qui détourne des informations.

²⁶ On trouve incidemment un autre exemple, saisissant par son caractère draconien de cette proximité entre «ce qu'on sait» et ce que l'on est physiologiquement dans l'Ancien Testament, au livre des Juges 12:5-6. Parce qu'ils ne pouvaient sur demande prononcer correctement un son qui n'existait pas dans leur propre langue, 42 000 Ephraïmites qui se prétendaient Galaadites auraient été égorgés.

Il s'agit donc d'une typologie pratique, et à laquelle on recourt ici dans cette mesure, mais qui devrait être affinée pour correspondre plus précisément à la réalité.

2- les caractéristiques recherchées

Quel que soit le type d'identifiant utilisé, celui qui veut identifier en souhaite l'efficacité et l'efficience; il doit donc comporter un certain nombre de caractéristiques qui le rendront utile. On peut notamment relever les éléments suivants à l'égard d'un type d'identifiant donné²⁷:

- l'identifiant devrait pouvoir servir à l'égard de chaque personne dans la population visée;
- l'identifiant spécifique devrait être propre à une seule personne, et chaque personne ne devrait avoir qu'un identifiant;
- l'identifiant devrait être précis, et donc empêcher la confusion entre personnes;
- l'identifiant ne devrait pas être modifiable et ne devrait pas avoir à être modifié;
- l'identifiant devrait être exclusif, de sorte qu'on n'aurait besoin d'en détenir aucun autre;
- l'identifiant devrait être indispensable, i.e. qu'on ne pourrait pas ne pas le détenir;
- l'identifiant devrait être pratique, de sorte qu'on pourrait l'utiliser facilement;
- l'identifiant devrait être «lisible», utilisable par toute personne autorisée dans tous les cas où cela paraît nécessaire;
- l'identifiant ou, du moins, sa trace, devrait être susceptible de conservation et de traitement;
- l'identifiant devrait être simple à utiliser de manière efficace;
- l'identifiant devrait être peu coûteux;
- l'identifiant devrait être socialement acceptable.

La première difficulté vient évidemment du fait que bien peu d'identifiants se conformant aux onze (11) caractéristiques précédentes se conformeront aussi à la douzième... En fait et comme on le saisira *infra*, l'identifiant-miracle n'existe pas encore. Envisagés individuellement, peu d'identifiants sont à la fois universellement détenus, précis, fixes et indispensables, par exemple. Le code génétique correspond relativement bien à ces critères, mais il n'est ni pratique, ni facile à utiliser, ni largement accepté dans la société.

²⁷ Cette nomenclature est inspirée de Clarke, *op. cit.*

III- L'authentification et le banquier

A- L'obligation d'authentifier

Les banquiers se plaisent à se définir à titre de «gestionnaires de risques». Il est vrai que certains clients leur confient une épargne qu'ils veulent récupérer, et que les banquiers mettent à leur tour les fonds qui leur sont confiés à la disposition d'autres clients, dont ils escomptent évidemment être remboursés. Les risques foisonnent donc dans l'activité bancaire, et ils ont souvent trait à l'authentification afin d'autoriser une personne préalablement identifiée à effectuer une opération.

Le banquier canadien doit d'abord identifier son client. Les règles visant à réprimer le recyclage des produits de la criminalité imposent en effet aux banquiers un certain nombre d'obligations quant à la détermination de l'identité juridique de la personne qui veut ouvrir un compte ou qui effectue certaines opérations²⁸. Le banquier veut aussi identifier son client «commerciallement», pourrait-on dire, afin notamment d'établir le profil de ses besoins mais aussi dans certains cas, comme l'attribution de crédit, de sa capacité financière.

Ce processus d'identification ne pose dans la plupart des cas aucun problème particulier: il est bien maîtrisé par les institutions financières traditionnelles et bien connu de la plupart de leurs clients²⁹. On requerra par exemple lors d'une ouverture de compte certains documents d'identité, qu'on examinera³⁰, et on demandera au nouveau client de répondre à des questions permettant de cerner les services dont il pourrait avoir besoin. Au besoin, et selon la nature des opérations, et notamment en matière de crédit, on tentera aussi d'établir la réputation du client, en vérifiant par exemple son dossier ou son score de crédit³¹.

Il faut toutefois noter que certaines institutions, comme la Banque ING, qui n'exploitent pas de succursale ou d'autre agence ayant pignon sur rue et où on peut ouvrir un compte (ou très peu), doivent recourir à une procédure un peu plus compliquée pour

²⁸ On pense notamment ici à l'article 14 du *Règlement sur le recyclage des produits de la criminalité et le financement des activités terroristes*, DORS 2002-184.

²⁹ Il faut néanmoins signaler qu'il subsiste une partie de la population qui ne dispose pas des identifiants généralement requis, et qui peut donc éprouver des difficultés à obtenir les services bancaires les plus essentiels. Ce problème s'est cependant atténué nettement depuis l'entrée en vigueur du *Règlement sur l'accès aux services bancaires de base*, DORS/2003-184.

³⁰ et on notera peut-être parfois le numéro qui y est associé, mais c'est une autre problématique.

³¹ Ces instruments posent eux-mêmes des problèmes particuliers en matière de protection des renseignements personnels, qui excèdent toutefois le champ de la présente étude.

procéder à l'identification de leurs clients³². Elles y parviennent néanmoins sans trop de peine et ce n'est pas à cet égard que les technologies biométriques retiennent principalement l'attention.

Une fois l'individu identifié et accepté à titre de client par l'institution financière, il voudra effectuer plus ou moins régulièrement des opérations, et c'est là que les choses se compliquent. Il s'agit en effet de contrôler épisodiquement que la personne qui désire procéder à une opération avec son banquier est bien celle qui y est autorisée: il faut authentifier ce requérant. Les risques associés, et donc les motifs de cette authentification, varient quelque peu selon le type d'opération, comme on le verra. Dans tous les cas toutefois, le banquier ressent la nécessité d'authentifier l'identité particulière d'une personne qui exprime la volonté de procéder à une opération.

B- Les modalités de l'authentification

On disait traditionnellement du banquier qu'il a vocation à accepter des dépôts, à honorer des chèques et à consentir des prêts³³. D'autres entreprises que les banques, au sens strict, offrent certes des services similaires, mais cette description générique conviendra pour nos fins. La forme de ces opérations a par ailleurs bien évidemment changé au fil des ans, ce qui explique qu'on recherche activement de nouvelles méthodes pour authentifier les gens, parce qu'il s'agit d'une étape cruciale dans la prestation du service fourni par le banquier.

Les raisons pour lesquelles cette opération importe tant varient quelque peu selon qu'on examine les cas du dépôt et du paiement, d'une part, ou du crédit, d'autre part. On brosera d'abord un tableau global de ces types de situations et des risques qu'elles comportent, puis on examinera en quoi la façon dont on effectue des dépôts, des paiements et des prêts change, avec d'inévitables conséquences sur les besoins liés à l'authentification.

³² Quant à cette institution en particulier, on visitera le www.ingdirect.ca/fr/openaccount.html pour se faire une idée des procédures d'ouverture mises en place.

³³ *United Dominion Trust Ltd. v. Kirkwood*, [1966] 1 All E.R. 968, 975 (C.A. R.-U.). On n'abordera pas ici la question extrêmement épineuse de déterminer ce qui constitue une activité proprement «bancaire» au sens de l'article 91 de la *Loi constitutionnelle de 1867* ou de la *Loi sur les banques*, L.R.C., c. B-1.1, question à l'égard de laquelle on lira par exemple Binavince, Emilio; Fairley, H. Scott. *Banking and the Constitution: Untested Limits of Federal Jurisdiction*. [1986] 65 R. du B. can. 328.

1- le «dépôt» et le paiement

Le consommateur confie volontiers son épargne au banquier (quand il en a). Il veut cependant être assuré que ce pécule ne sera en aucune circonstance capté sans droit par un tiers.

Il faut évidemment opérer ici une distinction entre les questions reliées à la sécurité physique, que nous écartérons, et celles qui nous intéressent. On examinera ensuite en quoi le cadre juridique applicable au Canada impose à bon droit au banquier d'authentifier soigneusement la personne qui lui transmet un ordre.

D'abord, évidemment, le consommateur préfère que son banquier ne soit pas victime d'un cambriolage, i.e. d'un acte par lequel une personne prélève sans droit du numéraire. Les mesures visant à contenir ce risque tiennent par exemple à la présence de vitres pare-balle dans les agences ou à la qualité des coffres-forts, et nous intéressent d'autant moins ici que le pillage de la banque n'a en principe aucune incidence juridique sur les droits du client qui y a effectué un «dépôt»³⁴.

C'est qu'il est admis en droit bancaire, au Québec comme ailleurs au Canada (suivant en cela le droit britannique), que l'opération qu'on qualifie vernaculairement de «dépôt» constitue en fait un prêt: le client prête de l'argent au banquier, à charge par ce dernier d'en remettre tout ou partie à ce client selon ses instructions³⁵. En droit civil, il s'agit d'un simple prêt³⁶ (par opposition au prêt à usage) et donc l'emprunteur, i.e. l'institution financière, doit rendre non pas exactement le bien qui lui a été prêté, mais en remettre «autant, de même espèce et qualité»³⁷.

Pour nos fins, la difficulté se situe ailleurs: il s'agit de savoir qui peut effectuer un dépôt ou un retrait, ou émettre un ordre de paiement. L'authentification prend là une importance particulière, notamment dans les deux derniers cas.

³⁴ On fait ici abstraction du cas maintenant impossible en pratique où un vol de numéraire serait d'une ampleur telle qu'il rendrait l'institution insolvable: l'examen des bilans des institutions financières démontre à l'évidence que le numéraire ne constitue qu'une assez petite proportion de leur actif et de la valeur de leurs capitaux propres.

³⁵ Quant à la qualification du «dépôt» bancaire à titre de prêt, *Foley v. Hill*, (1848) 2 H.L. Cas. 28, 9 E.R. 1002; *Joachimson v. Swiss Bank Corp.*, [1921] 3 K.B. 110 (C.A.); *Bank of Ottawa v. Hood*, (1908) 42 R.C.S. 231; au Québec, *Corp. Agencies Ltd. v. Home Bank*, [1925] 4 D.L.R. 585, conf. [1927] 2 D.L.R. 1 (C.P.) et *A.G. Canada v. A.G. Quebec; Bank of Montreal v. A.G. Quebec*, [1947] 1 D.L.R. 81 (C.P.). Pour alléger le texte, on continuera néanmoins à recourir ici au vocable de «dépôt».

³⁶ *Code civil du Québec*, art. 2314.

³⁷ Le cambriolage n'affecte donc pas la portée de l'obligation du banquier, qui devra remettre à son client toute somme que ce dernier a déposée.

Il ne faudrait cependant pas croire que l'authentification ne comporte pas d'importance à l'égard du dépôt lui-même. D'abord et si les fonds sont égarés et par exemple imputés par mégarde au compte d'un tiers, le déposant voudra pouvoir prouver que c'est bien lui qui a déposé une somme donnée et que cette dernière devrait donc être inscrite à son crédit. Ensuite, le client veut dans tous les cas être assuré qu'il fait bien affaire avec son banquier, et non avec un usurpateur³⁸. Ce ne sont cependant pas ces cas qui suscitent le plus souvent la controverse.

La validité des opérations par lesquelles des fonds sont déduits du compte d'un client pose évidemment des problèmes plus épineux, au moins dans la perspective de ce dernier. Le client qui a effectué un dépôt souhaitera tôt ou tard récupérer des liquidités, ou ordonner à son banquier d'en expédier à un tiers que ce client veut payer³⁹. Le banquier désirera toutefois s'assurer que l'ordre de paiement émane bien de son client ou d'une personne que ce dernier a dûment autorisée à émettre de tels ordres: c'est que la tentation est grande pour certains escrocs de s'emparer de fonds qui sont dus à d'autres, et donc d'usurper l'identité particulière du client ou de son mandataire.

Puisque le banquier est le débiteur du prêt⁴⁰ que lui a consenti son client, il doit à la demande de ce dernier effectuer un remboursement, conformément aux modalités de la demande formulée⁴¹. Il incombe juridiquement au banquier de contrôler l'authenticité de l'ordre de paiement qu'il reçoit, puisque le décaissement effectué sans autorisation valide sera contraire aux obligations contractuelles du banquier et inopposable au client⁴². Le banquier devrait donc dans ce dernier cas remettre à son véritable client une somme qu'il a déjà versée par mégarde à un tiers, ce qui le rend susceptible d'encourir une perte s'il ne parvient pas à réclamer le montant en cause de ce tiers.

À l'inverse, le banquier qui refuse sans raison valable de se conformer à un ordre de retrait ou de paiement à un tiers dûment donné par un client commet une faute et

³⁸ Et la prolifération actuelle des pratiques d'hameçonnage (ou *phishing*) marque bien l'importance de cette problématique.

³⁹ ce qui est en définitive la fonction du chèque ou du paiement au point de vente par carte de débit, par exemple.

⁴⁰ et on s'intéresse évidemment ici surtout au prêt remboursable à demande, et non au prêt à terme, qui pose moins fréquemment des problèmes pratiques.

⁴¹ *Foley v. Hill, op. cit. Joachimson v. Swiss Bank Corp., op. cit.; Clansmen Resources v. Toronto-Dominion Bank*, (1990) 43 B.C.L.R. (2d) 273 (C.A.C.-B.). On présumera bien sûr ici qu'il se trouve bien des fonds dans le compte qui fait l'objet d'un ordre de retrait et que cet ordre est clair et précis.

⁴² *Bank of Montreal v. The King*, [1907] 38 R.C.S. 258. En matière de lettres de change tout particulièrement, la lettre ou, plus concrètement, la signature ou l'endossement contrefaits d'un chèque tiré sur un compte seront sans effet: *Loi sur les lettres de change*, L.R.C., c. B-4, art. 48-49.

encourt la responsabilité pour le préjudice qui serait occasionné au client⁴³. Le banquier désire donc éviter non seulement les situations où il se conformerait erronément à un ordre, mais aussi celles où sa non-conformité serait tout aussi erronée. Bref, il veut savoir avec le plus haut niveau de certitude possible qui lui donne un ordre de paiement ou veut exécuter un retrait⁴⁴.

Corrélativement, le client doit pour sa part prendre des précautions raisonnables afin de ne pas faciliter la confection d'ordres de paiement qui seraient frauduleux⁴⁵.

Classiquement, les banquiers ont eu recours à la vérification de la présence d'une signature connue et autorisée sur l'ordre de paiement⁴⁶ pour l'authentifier. Toutefois et comme on le verra *infra*, le recours à la signature à titre d'authentifiant pose des difficultés croissantes; le besoin de procéder à l'authentification ne s'atténue cependant pas.

Il s'agit donc ici pour le banquier de maîtriser un double risque juridique, celui de procéder à une opération non légalement autorisée ou de ne pas procéder à une opération qu'il devrait effectuer. Le premier se double d'un risque de liquidité. Dans tous les cas, l'erreur sera attribuable à une maîtrise insuffisante d'un risque d'exploitation et elle pourra se doubler de la création d'un risque réputationnel.

2- l'opération de crédit

Le crédit bancaire à la consommation prend principalement deux (2) grandes formes. En matière de crédit fixe, le consommateur consultera son banquier, qui acceptera de lui consentir un prêt d'un montant déterminé, qui sera le plus souvent décaissé en une seule opération au bénéfice de l'emprunteur: le prêt hypothécaire en constitue l'archétype. Il y aura habituellement rencontres et discussion entre le consommateur et son banquier, physiquement en présence l'un de l'autre⁴⁷. Ce dernier peut donc identifier sans difficulté

⁴³ Ogilvie, Margaret. *Canadian Banking Law*. Toronto, Carswell, 1991. 798 p. Pp. 542-543, et jurisprudence y citée.

⁴⁴ On se situe évidemment ici au niveau du principe, étant donné notamment qu'il est acquis que, dans le cadre du processus de compensation interbancaire et de traitement des chèques, les institutions financières ne vérifient pratiquement jamais l'authenticité des signatures figurant sur les chèques, s'en remettant à la vigilance de leurs clients pour assurer la détection d'éventuelles fraudes.

⁴⁵ *Young v. Grote*, [1827] 130 E.R. 764; *London Joint Stock Bank v. MacMillan*, [1918] A.C. 777 (C.P.).

⁴⁶ y compris le bordereau de retrait en agence.

⁴⁷ On n'ignore pas qu'on assiste présentement, aux États-Unis notamment, à l'essor de prêteurs accordant du crédit fixe sur l'Internet, qui font évidemment face à un problème délicat en matière d'identification de leur client. Il s'agit cependant d'un phénomène encore marginal au Canada, et les problèmes relèvent davantage de l'identification des clients que de leur authentification périodique à des fins

son cocontractant et il n'a à authentifier cette identification qu' aux moments de la décision d'accorder le prêt et du décaissement, généralement unique⁴⁸.

En matière de crédit variable au contraire, le consommateur peut obtenir des avances de fonds chaque fois que cela lui paraît opportun, et sans être en présence de son banquier. L'utilisation de la carte de crédit en fournit le plus remarquable exemple, mais l'accès à une facilité de crédit accessoire à un compte bancaire par l'entremise d'un guichet automatique ou d'un achat par carte de débit au point de vente suscite les mêmes problématiques. Le banquier veut évidemment s'assurer qu'il n'émet du crédit qu'à la personne même à qui il l'a consenti: il ne pourra en effet obtenir de remboursement de la part de son client à l'égard de sommes que le banquier aurait par mégarde, et sans faute du client, versées à un tiers.

Le scénario diffère donc notablement de celui du crédit fixe. Dans les deux cas, le banquier aura d'abord cherché à identifier son client, et notamment à établir son nom et ses autres caractéristiques personnelles, mais aussi sa capacité de rembourser le crédit consenti. En matière de crédit variable cependant, il faut de surcroît authentifier la personne chaque fois que quelqu'un veut recourir à une partie du crédit accordé, pour s'assurer que celle qui loge cette demande est bien autorisée à le faire.

C'est donc principalement un risque de crédit qu'encourt ici le banquier, qui découlerait d'une mauvaise maîtrise du risque opérationnel dans le cadre de l'authentification d'une demande d'autorisation. Bien sûr, il y a risque juridique et risque réputationnel, mais c'est la perte sèche attribuable à la fraude d'usurpateurs qui préoccupe principalement le banquier.

On saisit donc d'emblée les différences dans les profils de risque, qui ne mènent pas nécessairement au même résultat.

En cas d'opération non autorisée en matière de retrait ou de paiement, c'est le client qui cherchera d'abord à obliger le banquier à lui remettre les sommes qu'il a déposées et n'a pas affectées, quitte pour le banquier à les récupérer auprès de celui qui les a détournées sans droit. Pour échapper à sa responsabilité civile, le banquier devra

d'autorisation. Dans l'état actuel des choses et comme on le verra *infra*, les solutions biométriques ne s'avèreraient donc que très modérément utiles.

⁴⁸ On fait ici abstraction des situations où le consommateur déménage, par exemple, et où le banquier voudra mettre son dossier à jour, de sorte qu'il devra obtenir de nouveaux renseignements personnels et s'assurer qu'ils sont bien ceux relatifs à son client, et non à un tiers.

prouver qu'il a exécuté un ordre légitime. Il veut donc compliquer l'usurpation d'un authentifiant.

La portée des efforts du banquier pourra toutefois varier: au Royaume-Uni, par exemple, les tribunaux ont tendu à admettre l'argument bancaire que la fraude par guichet automatique sans la complicité du consommateur détenant une carte et un numéro d'identification personnel était impossible. Les banquiers ont donc réduit leurs efforts en matière de lutte à la fraude, puisque ce sont les consommateurs qui écopaient, en laissant subsister des risques d'exploitation d'une ampleur déconcertante⁴⁹. Les tribunaux états-uniens ont eu tendance à adopter l'attitude inverse, et le comportement des banquiers s'est traduit par la mise en place de mesures anti-fraude (en principe) plus efficaces. En somme, la variation locale dans l'ampleur du risque juridique a eu des retombées sur les modes de gestion du risque opérationnel.

En matière de crédit, par contre, et notamment de crédit variable, c'est d'abord le banquier qui cherchera à être remboursé de prêts qu'il n'a pas versés à la bonne personne⁵⁰. Il ne dispose de pratiquement aucun moyen pour déplacer ce risque de perte vers un tiers (sinon son assureur).

C- L'évolution des marchés

Il y a trente (30) ans à peine, les Canadiens effectuaient leurs dépôts ou leurs retraits bancaires au comptoir de l'agence, et ils payaient en numéraire, par chèque ou, quand c'était par carte de crédit, en apposant leur griffe sur une facturette. La signature manuscrite régnait donc en maîtresse en matière d'authentification et, qui plus est, le

⁴⁹ Anderson, Ross. *Why Cryptosystems fail*. Cambridge, 1993. Disponible au www.ftp.cl.cam.ac.uk/ftp/users/rja14/wcf.pdf Par exemple, le système d'exploitation des guichets automatiques d'une banque britannique comportait cette étrange caractéristique que lorsqu'on insérait dans un guichet une carte d'appel téléphonique, le guichet présumait qu'on avait réinséré la dernière carte bancaire qu'on y avait utilisé. Certains guichets d'une autre banque britannique livraient automatiquement dix (10) billets de banque lorsqu'une certaine séquence de 14 chiffres était tapée au clavier de l'appareil, or cette séquence avait été divulguée dans le manuel d'exploitation diffusé dans toutes les succursales... Le catalogue des risques de sécurité associés aux réseaux de guichets automatiques (à tout le moins au Royaume-Uni au début des années 1990) que recense l'auteur ne manque pas d'étonner.

⁵⁰ Bien sûr et dans les cas où des opérations de crédit variable frauduleuses auraient par exemple épuisé le crédit disponible, le consommateur qui est le véritable emprunteur, et à qui on dénie tout à coup le crédit auquel il a droit en principe, voudra agir contre son banquier. Il s'agit toutefois d'un problème conceptuellement accessoire à la difficulté principale, même s'il peut bien sûr s'avérer fort épineux pour le consommateur qui en fait les frais.

client qui visitait son agence bancaire deux fois par mois ou plus en moyenne⁵¹, y était souvent physiquement reconnu par le personnel.

Les choses ont bien changé. Les Canadiens ont effectué plus de deux milliards et demie (2,5 G) d'opérations de paiement au point de vente par l'entremise de réseaux partagés en 2005, et deux cent quatre-vingt douze millions (292 M) retraits par guichet automatique partagé⁵². Le nombre de chèques de moins de cinquante mille dollars (50 000\$) traité par le système de compensation interbancaire diminue d'année en année⁵³.

Pour leur part, les opérations par carte de crédit sont maintenant souvent réalisées sans aucune signature manuscrite, puisque les parties ne se trouvent pas physiquement en présence l'une de l'autre.⁵⁴ Le volume d'opérations effectué par des membres de Visa Canada a augmenté en moyenne d'un peu moins de quinze pour cent (14,5%) par année chaque année depuis 1995 et la valeur de ces opérations a quant elle crû en moyenne d'un peu plus de onze pour cent (11,2%) par an chaque année durant la même période, pour atteindre cent quarante-six milliards de dollars (146 G\$) en 2005⁵⁵.

Le volume de paiements effectués sur l'Internet traités par les membres de Visa Canada atteindrait maintenant plus de six pour cent (6,2%) du volume total des opérations par carte Visa au pays, soit un peu plus de huit milliards de dollars (8,3 G\$) en 2005. Plus de cinq millions (5 M) de détenteurs de cartes Visa auraient effectué au moins un

⁵¹ En 1998 encore, les consommateurs québécois effectuaient physiquement des opérations bancaires au comptoir de leur institution financière 2,6 fois par mois en moyenne: CROP Inc. *Étude sur les transactions bancaires et les frais encourus par les consommateurs*. Montréal, CROP inc., février 1998. Question 23. L'échantillon du sondage était de 1 000 personnes et la marge d'erreur était de 3%, 19 fois sur 20.

⁵² Association canadienne des paiements. *Débit annuel des effets de paiement passant par le système automatisé de compensation et de règlement (SACR)*. Ottawa, Association canadienne des paiements, 2006. Les données diffèrent légèrement de celles fournies par Interac parce que ce réseau, même s'il est nettement le plus connu, n'est pas le seul réseau de guichets partagés et que toutes les opérations de paiement au point de vente ne passent pas par la compensation interbancaire. On trouve ces statistiques relatives aux opérations traitées par le système de compensation interbancaire canadien, qui ont la grande qualité de constituer une série continue depuis 1983, au www.cdnpay.ca/publications/acss_ann_fr.asp.

⁵³ Le nombre de ces chèques a diminué de 18,3% de 2000 à 2005: *ibid.*

⁵⁴ Et même en l'absence de la carte elle-même: c'est le cas des opérations sur l'Internet, mais aussi des appareils qui utilisent la technologie RFID pour «authentifier» par exemple le détenteur d'une carte de crédit et, surtout, de l'objet agité près de la pompe à essence qui permet de conclure l'opération de paiement sur carte de crédit sans aucune autre formalité, comme le *Speedpass* déployé par la Compagnie pétrolière Impériale et les produits similaires de certains de ses concurrents.

⁵⁵ Visa Canada Association. *2005 Corporate Report*. Toronto, Visa Canada Association, 2006. 40 p. Pp. 32-33. Disponible au <http://corporate.visa.com/av/pdf/VisaCanadaReport.pdf>.

paiement sur l'Internet avec leur carte en 2005⁵⁶. Le réseau MasterCard affiche vraisemblablement une croissance comparable.

Pour sa part, le groupe Interac offre depuis le mois de décembre 2005 un mécanisme de paiement qui permet à l'internaute de faire un paiement au bénéfice d'un commerçant à partir des fonds se trouvant dans son compte bancaire⁵⁷, le tout bien sûr sans signature manuscrite.

Ailleurs dans le monde, le téléphone mobile paraît en passe de devenir lui aussi un instrument d'authentification à des fins de paiement. Les cartes prépayées percent également certains marchés⁵⁸.

En somme et pour emprunter à l'Association Visa Canada,

«Today, over half of all consumer transactions in Canada are completed using some means of electronic payment. By comparison, just over ten years ago, roughly 80% of all consumer transactions in Canada, by dollar volume, were completed using cash or cheque. Over time, Visa Canada's share of spending in Canada has grown steadily and represents 16% of all consumer spending».⁵⁹

Bien sûr, le numéraire n'est pas encore disparu, encore que certains s'évertuent à prédire qu'il ne circulera plus d'ici une décennie⁶⁰. Le consommateur canadien moyen détiendrait environ soixante-dix dollars (70 \$) dans son porte-monnaie et le numéraire demeurerait son moyen de paiement favori pour les opérations d'une valeur de moins de vingt-cinq dollars (25 \$)⁶¹. Le numéraire comporte quand même toujours certains avantages, dont son caractère pratique, l'irrévocabilité du paiement, la sécurité inhérente et l'anonymat qu'il permet.

⁵⁶ *Ibid.*, pp. 2, 15, 28.

⁵⁷ Il s'agit du service *Interac en ligne*, à l'égard duquel on consultera le www.interacenligne.com.

⁵⁸ Au Canada, Visa Canada s'intéresse notamment à ce créneau: *op. cit.*, p. 28.

⁵⁹ *Ibid.*, p. 9. L'Association ne cite malheureusement aucune source à l'égard de ces données.

⁶⁰ Pour des itérations relativement récentes de cette prophétie récurrente, on verra par exemple *TowerGroup Envisions a Cashless Society by 2015*, Epaynews.com, 15 février 2006; *Is the End of Cash at Hand?*, Bank Systems & Technology online, 28 septembre 2005, au www.banktech.com/showArticle.jhtml?articleID=17120571; Harper, Rebecca. *The New Currency – Kiss you cash good-bye. By 2010, two-third of your payments will be virtual*. Wired, avril 2004, p. 59.

⁶¹ Taylor, Varya. *Tendances en matière de paiement de détail et résultats d'un sondage mené auprès du public*. Revue de la Banque du Canada, printemps 2006, p. 27.

Dès qu'on passe à des opérations de plus de quelques dizaines de dollars, non seulement le numéraire, mais la signature manuscrite, qu'on peut associer à un élément d'authentification relatif à «ce qu'on est», et donc biométrique, paraît nettement en perte de vitesse, parce qu'elle est relativement mal adaptée aux opérations à distance. On l'a dans une large mesure remplacée par le recours à des mots de passe ou des «numéros d'identification personnelle», et donc à «ce qu'on sait», et à la détention d'objets, comme des cartes.

Cette évolution s'est accompagnée d'une certaine mutation dans l'allocation des risques entre le banquier et son client, dont il faut maintenant dire un mot.

D- L'allocation des risques

Le passage de la signature au numéro d'identification personnel s'est dans une certaine mesure doublé d'une étrange évolution juridique, où l'absence de responsabilité du consommateur à l'égard de la contrefaçon d'un identifiant essentiellement public s'est graduellement mutée en responsabilité onéreuse en raison de la contrefaçon d'un identifiant essentiellement secret. La comparaison avec la responsabilité du banquier en ce qui a trait au chèque permet de mieux saisir ce mouvement.

Historiquement et dans les juridictions s'inspirant de la *common law*, la signature contrefaite sur un chèque ne peut avoir aucun effet juridique⁶². Le banquier qui a honoré un chèque qui n'avait pas véritablement été signé par le tireur doit intégralement rembourser ce dernier et court donc le risque d'une perte, puisqu'il ne pourra qu'exceptionnellement récupérer la somme payée au fraudeur. La solution tombe cependant sous le sens, puisqu'il appartient au banquier de vérifier la signature sur l'effet qu'il encaisse et qu'il dispose des moyens qui lui permettent de le faire. Le fardeau de démontrer l'authenticité de la signature portée sur l'effet repose sur le banquier et ce n'est que s'il en administre une preuve *prima facie* que le client devra présenter une réfutation. Et il semble que les expertises dans ce domaine permettent d'en venir à un assez haut degré de certitude quand à l'authenticité d'une signature⁶³.

⁶² C'est au Royaume-Uni l'effet de l'article 24 du *Bill of Exchange Act* (1882) et, au Canada, de l'article 48 de la *Loi sur les lettres de change*, L.R.C., c. B-4. La problématique est analysée dans Bohm, Nicholas; Brown, Ian; Gladman, Brian. *Electronic Commerce: Who Carries the Risk of Fraud?* 2000 (3) *Journal of Information, Law and Technology*, dont on trouvera le texte au <http://elj.warwick.ac.uk/jilt/00-3/bohm.html>.

⁶³ *Ibid.*

On assiste avec l'essor de la carte de crédit et de la carte de débit à une tentative de la part des banquiers de faire porter la responsabilité de toutes les opérations sur le consommateur. La même tendance se manifeste dans certains cas à l'égard des opérations bancaires en ligne. Ce serait après tout sa faute s'il a divulgué son NIP ou laissé traîné sa carte. Parce qu'on prétend imposer le secret et la sécurité à l'égard de ces identifiants, et puisqu'une faille ne pourrait provenir que de la faute de leur détenteur, ce dernier devrait payer le prix de l'opération frauduleuse.

Fort heureusement, la législation et, dans une bien modeste mesure, des codes de conduite, viennent refréner cette propension des banquiers à se délester de leur responsabilité, au moins à l'égard des opérations par carte de crédit et de débit⁶⁴. Il faut après tout prendre en compte ce détail que ce sont eux qui ont conçu et qui gèrent des systèmes de paiement dont ils savent mieux que quiconque la médiocre fiabilité. Il faut aussi s'étonner que dans un contexte où une information constitue forcément un secret partagé⁶⁵, la responsabilité du bris du secret soit présumée dans tous les cas retomber sur les épaules d'une seule des parties⁶⁶.

On ne peut d'autre part que déplorer que des commerçants invoquent les failles de processus d'authentification qu'elles ont mis en place, comme la difficulté pratique de maintenir le secret d'un NIP, pour faire porter la responsabilité d'une opération frauduleuse sur la partie à l'opération qui se trouve structurellement placée dans la position la plus faible. L'échec de la dissimulation d'un NIP ne résulte jamais autant de la négligence d'un consommateur⁶⁷ que de la mauvaise conception d'un système d'authentification.

Un cadre normatif qui n'interdit pas à ceux qui conçoivent et implantent des processus d'authentification déficients de déplacer contractuellement vers d'autres parties moins bien informées la plus grande part des risques associés aux lacunes de ces systèmes n'incite évidemment pas à l'amélioration de ces processus. Les autres parties – et

⁶⁴ Il faut cependant signaler que les banquiers s'efforcent de repousser une part de la responsabilité que la loi épargne aux consommateurs vers les commerçants. Dans le cas d'opérations par carte de crédit sur le web, et donc où le consommateur n'a pas apposé sa signature à une autorisation de paiement, le contrat entre son banquier et le commerçant imposera en effet souvent à ce dernier de subir la perte associée à un achat non autorisé: Bohm *et al.*, *op. cit.*, qui décrivent plus précisément le cadre juridique et les pratiques bancaires au Royaume-Uni.

⁶⁵ puisque le NIP doit pouvoir être validé par l'institution financière, elle doit le connaître ou connaître, du moins, une information qui en est dérivée – mais elle connaîtra aussi forcément le processus de dérivation, et donc elle peut vraisemblablement reconstituer l'information.

⁶⁶ Bohm *et al.*, *op. cit.*

⁶⁷ qu'on présumera ici de bonne foi, les cas de fraude délibérée relevant d'une autre problématique.

notamment les consommateurs – font les frais des coûts découlant des dérèglements occasionnels et les tolèrent, compte tenu des avantages que leur procurent par ailleurs les systèmes dont ces modes d'authentification sont les accessoires. On ne saurait toutefois exclure que leur patience s'épuise un jour. D'ici là, la société entière fait au fond les frais de systèmes moins efficaces qu'ils ne pourraient l'être, parce que ceux qui peuvent les mettre en place n'en voient pas l'avantage à court terme. Ainsi va le marché...

E- Les méthodes d'authentification

1- la signature

Pour qu'il y ait contrat, il faut des personnes accordant leur consentement. Elles ne sont pas toujours requises de s'identifier⁶⁸, mais elles le feront parfois, et ce d'autant que la valeur de l'opération est élevée.. Elles pourront d'autre part vouloir conserver pour l'avenir une preuve du contenu de l'accord: l'écrit s'est traditionnellement imposé à cette fin⁶⁹. Et, pour attester du consentement du cocontractant, on a notamment recouru depuis des millénaires à l'apposition écrite de son nom par la personne elle-même, i.e. à sa signature⁷⁰.

La signature manuscrite comporte intrinsèquement deux (2) caractéristiques: d'une part, elle constitue implicitement la déclaration par le signataire qu'il peut s'identifier sous le nom qu'il indique: si ce n'est pas le cas, le signataire fournit la preuve de sa volonté de tromper autrui, et il commet une fraude. Ensuite, la forme de la signature se trouve intimement rattachée à un individu donné (sous réserve de contrefaçon): chacun signe à sa manière. L'autographe s'avère bien l'écriture de soi par soi.

Dans la forme et dans le fond, la signature identifie par conséquent une personne en particulier et peut de plus être conservée⁷¹. On ne s'étonne donc pas qu'il s'agisse d'une

⁶⁸ D'innombrables contrats, comme la vente d'un café ou du journal du matin, ou la commande d'épicerie payée comptant, sont conclus sans que le consommateur s'identifie.

⁶⁹ qu'il soit gravé sur lapierre ou bien couché sur le papyrus ou le vélin.

⁷⁰ La signature manuscrite est assurément connue du droit romain. Les Saxons qui sont entrés en Angleterre dans les derniers siècles de l'Empire romain utilisaient la signature, mais son usage fut pendant une longue période remplacé en Grande-Bretagne par le recours au sceau, avant que la signature manuscrite redevienne un élément essentiel de la conclusion de certains contrats au 17^e siècle: Blackstone, William. *Commentaries on the Laws of England*. Vol. 2. A Facsimile of the First Edition of 1765-1769. Chicago, The University of Chicago Press, 1979. 520 p. Pp. 305-306.

⁷¹ Notons à cet égard et en corollaire un détail auquel on reviendra: si importante qu'elle soit à titre d'identifiant ou d'authentifiant, la signature n'est pas secrète. Elle peut donc assez facilement être

fort vieille invention, mais qu'elle soit aussi encore utilisée couramment à titre d'identifiant. Dans le contrat écrit ou dans l'acte matériel qui vise à prouver une opération, l'identité des parties se trouve alors apparemment ramenée à leur signature. On identifie, au sens de «confondre», la personne et le signe.

La signature comporte toutefois des difficultés. D'abord, elle laisse justement la trace du nom de l'individu, qui pourrait préférer ne pas fournir précisément cette information. Ensuite, elle peut être imitée relativement facilement, puisqu'elle est évidemment assez largement connue et qu'il suffit d'une certaine habileté manuelle pour la contrefaire. Elle est d'autre part pratiquement réservée aux gens qui peuvent écrire⁷².

À titre d'authentifiant, la signature recèle d'autre part l'immense défaut qu'elle requiert une comparaison entre l'autographe de la personne qu'on veut reconnaître, d'une part, et un modèle compilé au moment de l'identification de la personne auprès de celui qui veut maintenant contrôler celui qui affirme être cette personne. Or, d'une part, la signature change, et parfois considérablement et rapidement, de sorte qu'il faut tenir à jour le registre de contrôle, avec les coûts qui en découlent ou le risque d'erreur⁷³. En plus, la comparaison requiert ou bien que l'individu effectue ses opérations là où le modèle de contrôle est détenu, ou bien qu'on rende ce modèle consultable à distance dans un réseau: ce processus demeurerait jusqu'à récemment coûteux et il a évidemment le défaut de permettre potentiellement à quiconque a accès au réseau de capter des signatures qui y sont disponibles, pour les contrefaire.

Ensuite, et bêtement, le contrôle de la signature exige... que l'on signe, et cette formalité paraît à la fois difficile à réaliser dans le cadre d'opérations à distance, comme sur l'Internet⁷⁴, et impose des frais et divers inconvénients. Par exemple et même en matière de paiement en personne par carte de crédit, la signature requiert du temps, et donc contribue à l'allongement de la file d'attente au supermarché; elle requiert aussi qu'on crée un document, puis qu'on l'archive. On ne s'étonne donc pas outre mesure que le

imitée d'une manière qui s'avérera convaincante au moins *prima facie*, et pourtant on y recourt sans hésitation pour authentifier des opérations financières considérables.

⁷² Certaines personnes sont physiquement incapables d'écrire et, surtout, une proportion encore significative de la population est très peu à l'aise avec l'écrit.

⁷³ Certains individus ont d'autre part une signature qui change constamment, ce qui compromet parfois l'authentification et conduit au rejet d'une demande par ailleurs valide.

⁷⁴ On fera ici abstraction du concept de «signature électronique», qui relève en soi d'une problématique qu'on ne peut explorer ici, ainsi que de la possibilité de munir un ordinateur ou un autre système informatique d'une «tablette» électronique sur laquelle on peut signer avec un stylet, comme le font par exemple certaines entreprises de messagerie, cette dernière méthode requérant potentiellement de la part de millions de consommateurs l'achat d'un matériel dont tous préféreraient faire l'économie.

groupe VISA ait annoncé aux États-Unis que dans ce pays, désormais, l'exigence de la signature sera tout simplement abolie pour les achats de moins de vingt-cinq dollars (25 USD)⁷⁵. Afin de rendre le mode de paiement plus attrayant, les institutions émettrices paraissent donc disposées à accepter dans une certaine mesure le risque que surviennent des opérations frauduleuses qui ne pourront être authentifiées par la signature du détenteur de la carte.

En somme, la signature, dans sa conception traditionnelle ne se prête pas bien aux opérations à distance et aux opérations électroniques et on a donc cherché à lui trouver des substituts.

2- le modèle de la clé

‘Got it,’ said Hagrid at last, holding up a tiny golden key.

The goblin looked at it closely.

‘That seems to be in order.’⁷⁶

Il n'est pas toujours nécessaire d'identifier quelqu'un au moment où on veut l'autoriser à effectuer une opération. Par exemple, la détention de la clé de la serrure permet d'entrer dans la maison. On présume alors que les modalités de sécurité entourant la conservation de la clé garantissent que seul un détenteur autorisé pourra l'utiliser.

On utilise abondamment le modèle de l'objet détenu pour authentifier une demande d'autorisation. Outre la clé traditionnelle, on peut songer à la carte magnétique qui permet l'accès au bureau ou à celle qui atteste du droit de conduire une voiture. La carte de crédit ou la carte de débit jouent aussi ce rôle⁷⁷.

Cette méthode d'authentification comporte cependant des inconvénients. D'abord, elle atteste le plus souvent non pas l'identité particulière d'une personne, mais son appartenance au groupe des détenteurs de l'objet en cause. L'objet peut en effet être dans certains cas prêté, il peut le plus souvent être volé et il peut être contrefait ou, tout simplement, égaré, avec aussi dans ce dernier cas des conséquences parfois fâcheuses pour le détenteur autorisé.

⁷⁵ *Visa To Drop Signatures For Low-Dollar Purchases*. Epaynews.com, 13 avril 2006.

⁷⁶ Rowling, J.K. *Harry Potter and the Philosopher's Stone*. Vancouver, Raincoast Books, 1997. 223 p. P. 57.

⁷⁷ Totalement ou en partie, selon le cas.

La seule utilisation de «ce qu'on a» pour authentifier une identification ou une autorisation n'est donc que modérément fiable. On combine donc souvent l'objet à autre chose, qu'il s'agisse d'une caractéristique d'ordre biométrique tenant à ce «qu'est» la personne (comme une photographie ou une signature) ou d'une caractéristique reliée à ce que sait la personne. On dira d'abord un mot de ce dernier modèle, avant d'aborder la problématique de la combinaison «objet – savoir».

3- le modèle du mot de passe

La détention d'une information permet fréquemment d'être autorisé à faire quelque chose. Il peut s'agir du code permettant l'ouverture d'une porte ou d'un coffre-fort, du numéro d'identification personnelle rattaché à un compte bancaire ou du mot de passe permettant l'accès à un réseau informatique. Ce modèle est actuellement abondamment utilisé dans nos sociétés, et notamment dans le secteur financier.

Il comporte pourtant des difficultés importantes. D'abord, on présume le plus souvent du secret de l'information qui sert à authentifier, sans quoi le contrôle est évidemment inutile: si tout le monde connaît le code ou peut le deviner facilement, il ne sert à rien d'en vérifier l'expression. Or le maintien du secret ne va pas de soi. Il faut en effet établir l'équilibre entre les mesures prises pour empêcher des personnes non agréées d'obtenir l'information-clé, d'une part, et le besoin que les personnes agréées puissent, elles, utiliser cette information. Le secret si abscons qu'il ne peut être connu ou, en pratique, mémorisé, par les personnes autorisées ne sera peut-être jamais deviné par des imposteurs (et encore), mais il sera aussi inutilisable par ceux pour qui il doit faire office de sésame⁷⁸.

Or le secret est facilement compromis. La personne non autorisée, mais habile au plan psychologique, pourra parfois l'obtenir d'un détenteur qui lui fait trop confiance. Il peut être noté, et donc lu. Il peut être intercepté, de diverses manières selon la façon dont il est utilisé à des fins d'authentification⁷⁹. Il peut être deviné, et souvent plus facilement

⁷⁸ Plus d'un citoyen britannique sur quatre éprouverait de la difficulté à se souvenir de ses divers modes de passe et numéros d'identification personnels: *Chip and PIN Effecting Change in Payment Habits*. The Times, 10 août 2004, repris sur epaynews.com, 13 août 2004.

⁷⁹ On connaît les espionciels qui peuvent enregistrer toutes les frappes sur un clavier d'ordinateur, mais on se souvient aussi de ces brigands qui avaient installé un faux guichet automatique dans un centre commercial des États-Unis il y a une douzaine d'années et avaient ainsi obtenu les numéros d'identification personnelle de centaines de consommateurs qui avaient tenté d'effectuer un retrait, ce qui leur a ensuite permis de contrefaire des cartes de guichet. Bien entendu, et plus simplement, il

qu'on le pense. Il devrait donc être modifié régulièrement pour préserver un haut niveau de sécurité, mais cela sera d'autant plus ardu qu'il doit être connu d'un grand nombre de personnes et qu'il est complexe. Et il peut être oublié par une personne autorisée, ce qui s'avère parfois ennuyeux.

La prolifération des situations où on recourt maintenant à une information pour authentifier une demande d'autorisation vient compliquer les choses. On recourt à des mots de passe ou des numéros d'identification personnelle un peu partout: le guichet automatique, l'accès à une zone du bureau, les accès à divers systèmes informatiques, l'utilisation de services différents sur l'Internet, la récupération des messages sur la boîte vocale associée à chaque téléphone... Les règles élémentaires de sécurité voudraient que le consommateur établisse dans chaque cas un mot de passe différent, comme on a des clés différentes pour la résidence, le chalet, le bureau ou sa voiture. En pratique, l'individu ne peut mémoriser facilement tant d'éléments différents, surtout s'ils sont très abstraits, comme «TY%9bvc72». Il utilisera donc souvent les mêmes, ou en choisira qui sont très faciles à mémoriser mais aussi, souvent, à percer.

La systématisation du recours à des secrets à des fins d'authentification paraît donc fondée sur une erreur conceptuelle, et se trouve par conséquent vouée à terme à l'échec. Les premiers systèmes de sécurité et de chiffrement déployés afin d'assurer la sécurité des réseaux de guichets automatiques, par exemple, s'inspiraient du modèle militaire, ce qui s'explique assez bien historiquement: la cryptographie, à laquelle on devait aussi avoir recours, s'était après tout surtout développée dans ce domaine au cours des décennies précédentes. Or le milieu militaire a une longue pratique de la gestion des secrets, qui ne se transpose peut-être pas si facilement dans la vie courante des consommateurs «civils». Comme l'indique un chercheur universitaire qui s'intéresse à ces questions,

«The first error may be largely due to an uncritical acceptance of the conventional military wisdom of the 1970's. When ATMs were developed and a need for cryptographic expertise became apparent, companies imported this expertise from the government sector. The military model stressed secrecy, so secrecy of the

suffit d'installer une caméra miniature et bien camouflée de telle sorte qu'elle pointe vers le clavier pour qu'on puisse saisir toute l'information voulue.

PIN was made the cornerstone of the ATM system; technical efforts were directed ensuring it, and business and legal strategies were predicated on its being achieved. It may also be relevant that the early systems had only limited networking, and so the security design was established well before ATM networks acquired their present size and complexity. Nowadays, however, it is clear that ATM security involves a number of goals, including controlling internal fraud, preventing external fraud, and arbitrating disputes fairly, even when the customer's home bank and the ATM raising the debit are in different countries. This was just not understood in the 1970's; and the need for fair arbitration in particular [sic] seems to have been completely ignored»⁸⁰.

On mesure bien les conséquences de ces méprises aujourd'hui. On condamne les citoyens à gérer un nombre croissant de secrets, avec les difficultés et les lacunes que cela comporte. On exploite des systèmes fondés sur une prémisse du secret qui s'avère peu réaliste, puis on tente trop de souvent d'imputer au consommateur la responsabilité d'un dérèglement du système⁸¹.

4- le modèle de l'apparence

En un sens, l'identification d'une personne par ce qu'elle est physiquement paraît la méthode la plus simple. Assurément, on y a communément recours, chaque fois qu'on reconnaît une personne connue à ses traits ou au timbre de sa voix. Sans doute est-ce la méthode d'identification la plus ancienne, la plus élémentaire. Le premier hic, c'est qu'elle ne suffit plus. Le second, c'est que d'aucuns voudraient lui prêter une fiabilité qui dépasse peut-être ses moyens.

⁸⁰ Anderson, Ross. *Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore*, Cambridge, 2002, 13 p. (note de fin de texte omise). On trouvera cette étude au www.net-security.org/article.php?id=145.

⁸¹ Les associations de consommateurs canadiennes savent en effet à quel point il peut parfois être difficile pour un consommateur d'obtenir gain de cause quand des retraits non autorisés ont été effectués dans son compte: son institution tentera de lui en imputer la faute, et les dispositions du *Code de pratique canadien des services de cartes de débit* lui seront trop souvent d'un secours relatif.

Les modes élémentaires d'identification par ce qu'on est conviennent évidemment dans des contextes «fermés»: des personnes qui se connaissent se reconnaîtront habituellement sans trop de peine lorsqu'elles se rencontrent, par exemple. Encore faut-il nuancer: des caractéristiques comme la couleur des cheveux, la voix, la posture... ne sont pas individuellement fiables et leur efficacité à titre d'identifiant dépend en bonne part de la mémoire de l'observateur⁸².

Des étrangers pourront éprouver plus de difficulté encore à cerner avec certitude les mêmes identifiants. Une simple description de la taille, de la couleur des cheveux ou des yeux (comme on la lit dans un passeport, par exemple), ne suffit pas à authentifier l'identité particulière d'une personne avec un degré significatif de fiabilité, raison pour laquelle on appose aussi dans le passeport la photographie du titulaire. C'est peut-être que les données morphologiques qu'on prend spontanément en compte pour «reconnaître» une personne à son apparence sont si nombreuses, et parfois si ténues⁸³, qu'elles défient presque la possibilité d'être décrites analytiquement: véritablement, ici, l'image vaut mille mots.

Pour mieux reconnaître un inconnu, beaucoup mettent alors l'accent sur la recherche d'un élément qui serait parfaitement individualisé: l'empreinte digitale ou rétinienne, certaines caractéristiques de la structure faciale seraient, dit-on, uniques, inimitables, immuables. Il s'agirait d'identifiants parfaits. L'examen de l'efficacité de ces technologies invite toutefois au scepticisme: en fait, leur fiabilité paraît moins qu'absolue.

Si ni l'objet, ni l'information, ni l'apparence ne constitue en soi un mode d'authentification parfaitement sûr et commode, la combinaison des deux modes permettrait-elle de bénéficier des qualités de chacune et d'atténuer les inconvénients des deux? C'est l'hypothèse qu'on pose maintenant aux États-Unis, notamment.

5- l'identification à deux facteurs

On assiste présentement, et notamment dans les milieux réglementaires encadrant le secteur financier aux États-Unis, à l'essor d'un courant: l'accent est mis sur l'authentification dite «à deux facteurs», notamment en matière d'opérations sur l'Internet.

⁸² Clarke, Roger. *Human Identification in Information Systems: Management Challenges and Public Policy Issues*. Canberra, Xamax Consultancy Pty Ltd., 1994. On trouvera ce document au [www.anu.edu.au/people/Roger.Clarke/DV/Humain ID.html](http://www.anu.edu.au/people/Roger.Clarke/DV/Humain%20ID.html).

⁸³ d'autant qu'on peut reconnaître non seulement la personne, mais jusqu'à un certain point ses états d'âme à un je-ne-sais-quoi dans le regard ou dans l'ampleur précise de la contraction de certains muscles zygomatiques, par exemple.

Cette tendance s'est notamment concrétisée par la publication le 12 octobre 2005 de lignes directrices publiées par le *Federal Financial Institutions Examination Council*⁸⁴.

Le *Council* entend par la notion de «facteur» le recours à «ce qu'on possède», «ce qu'on sait» ou «ce qu'on est». Il recommande très vivement aux institutions financières encadrées par ses membres qu'elles recourent à une combinaison de facteurs pour authentifier les opérations bancaires courantes:

«The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties».⁸⁵

De l'avis du *Council*,

«Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods».⁸⁶

Par conséquent, le consommateur ne devrait plus pouvoir consulter la section «transactionnelle» du site web de son institution financière en n'utilisant qu'un mot de passe, comme c'est souvent le cas présentement aux États-Unis comme au Canada. D'autres méthodes devraient être combinées à ce facteur informationnel qu'est le mot de passe ou le numéro d'identification personnel:

«There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public

⁸⁴ Federal Financial Institutions Examination Council. *Authentication in an Internet Banking Environment*. Arlington (VA), Federal Financial Institutions Examination Council, 2005. 14 p. (Ci-après «FFIEC»). Le *Council* regroupe les organismes réglementaires fédéraux des États-Unis en matière d'encadrement des activités bancaires ou quasi-bancaires. Les lignes directrices sont disponibles au www.ffiec.gov/pdf/authentication_guidance.pdf.

⁸⁵ *Ibid.*, p. 1.

⁸⁶ *Ibid.*, p. 3. On notera que le *Council* ne tente pas de quantifier dans quelle proportion cette difficulté pourrait être accrue et, s'il s'agit là d'un énoncé qui paraît logique au premier abord, on peut sûrement envisager des scénarios où, par exemple, la seconde méthode serait si peu commode à utiliser que de nombreux usagers la neutraliseraient et rendraient peut-être ainsi le processus encore plus vulnérable qu'avant que le second facteur d'authentification soit ajouté au système.

key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of “tokens”, transaction profile scripts, biometric identification, and others. [...] The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.»⁸⁷

On voit donc la panoplie de méthodes envisagées, dont les méthodes biométriques ne constituent qu'un élément. On saisit bien aussi qu'il s'agit de choisir la bonne combinaison, compte tenu de l'évaluation des risques mais, également, comme le note plus loin le *Council*, de l'évaluation des modes d'implantation et d'autres éléments:

«The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accomodate growth, and interoperability with existing systems and future plans».⁸⁸

On aurait également pu ajouter parmi ces éléments l'efficacité et la fiabilité des modes d'authentification choisis, qui sont fort délicats à pondérer.

Il est en effet parfois fascinant – et troublant – d'observer le contraste entre la perception que se font des autorités réglementaires, des institutions financières ou des fabricants de systèmes de sécurité, et celle que s'en font des experts en matière de sécurité ou d'informatique, en ce qui a trait à la quantification de l'ampleur du risque associé à l'usage de l'une ou l'autre méthode. Par exemple, le FFIEC avance que les cartes à puce

⁸⁷ *Ibid.*, p. 2.

⁸⁸ *Ibid.*, p. 3.

sont difficiles à contrefaire et *tamper resistant*⁸⁹; par contre, des auteurs spécialisés recensent une série de méthodes par lesquelles on peut attaquer une carte à puce⁹⁰.

De la même manière, le FFIEC souligne les grands avantages que peut comporter l'utilisation de ce qu'il est convenu d'appeler une «clé USB» à titre de facteur d'authentification et note là encore que ces outils sont *hard to duplicate and are tamper resistant*⁹¹, mais omet de noter que ces petits objets fort pratiques sont aussi très faciles à perdre ou à voler... Leur contribution véritable à l'exploitation sécuritaire et efficiente d'un réseau de communications, dans le secteur financier ou ailleurs, doit donc être relativisée dans cette mesure, qui n'est pas négligeable.

F- L'état des choses

La signature s'efface doucement. Les limites de la combinaison d'une carte et d'un mot de passe deviennent manifestes et, si la substitution d'un micro-processeur à la bande magnétique sur les cartes bancaires réduira sans doute un peu pour quelque temps la prévalence de la fraude, l'effet sera sans doute limité et on n'aura rien changé à ce qui constitue pour le consommateur une difficulté récurrente avec ce modèle, soit la gestion des mots de passe. D'autant que les banquiers ne requièrent pas de mots de passe que lorsqu'on emploie une carte, mais aussi quand on veut faire une opération sur l'Internet.

Malgré tout, l'activité frauduleuse tend à augmenter. Pour la réprimer, on songe à d'autres méthodes; celles qui relèvent de la biométrie peuvent paraître alléchantes puisqu'à en croire les promoteurs, il s'agirait de solutions pratiques et admirablement efficaces. À l'examen, la situation paraît cependant requérir beaucoup plus de nuances.

IV- L'authentification biométrique: un survol

A- Quelques illustrations

Certains clients d'un grand hôtel de Boston peuvent maintenant entrer dans leur chambre après une vérification de leur iris, au lieu d'utiliser une clé⁹². De plus en plus de

⁸⁹ FFIEC, *op. cit.*, appendice, p. 9.

⁹⁰ Schneier, Bruce; Shostack, Adam. *Breaking Up is Hard to Do: Modeling Security Threats for Smart Cards*. USENIX Workshop on Smartcard Technology, may 1999. Available at www.counterpane.com/smart-card-threats.html.

⁹¹ FFIEC, *op. cit.*, p. 8.

⁹² Kontzer, Tony. *Hotel's Guests Embrace Iris-Recognition Technology*. Information Week, 9 décembre 2004, au www.informationweek.com/story/showArticle.jhtml?articleID=55300787.

fabricants d'ordinateurs, dont la firme HP, équipent leur portable d'un lecteur d'empreinte digitale afin de contribuer à contrôler l'accès au contenu logique de la machine⁹³.

Les clients d'un dépanneur de Tampa, en Floride, n'ont qu'à mettre le doigt sur un lecteur pour effectuer des paiements, prélevés directement dans leur compte bancaire⁹⁴. La même méthode vient tout juste d'être implantée dans treize (13) postes d'essence du Missouri⁹⁵.

De grandes chaînes comme Wal-Mart et Costco envisagent aussi de recourir aux empreintes digitales à titre d'authentifiant pour effectuer des paiements à la caisse⁹⁶.

Des fournisseurs envisagent de mettre d'ici peu sur le marché des lecteurs d'empreintes digitales qu'un consommateur pourrait tout bonnement brancher à son ordinateur, comme tout autre équipement périphérique⁹⁷.

Au Pakistan et en Colombie, des guichets automatiques bancaires sont munis de lecteurs d'empreintes digitales⁹⁸.

En Utah, une institution financière permet à des clients d'encaisser des chèques en s'identifiant grâce à leur empreinte digitale⁹⁹. On sait qu'au Canada, la firme Insta-chèques prélève l'empreinte digitale des clients qui encaissent des chèques, encore qu'on ne sache trop ce qu'ils en font.

Ce n'est pas encore une vague. C'est toutefois un phénomène en émergence. Il faut dès maintenant en cerner la portée.

B- Des difficultés d'ordre général

Si l'identité d'une personne tient notamment à ce qu'elle est, l'examen de ses caractéristiques les plus personnelles devrait constituer le meilleur moyen d'établir à qui on a affaire. Hélas, les choses ne s'avèrent pas si simples en pratique, et ce pour plusieurs raisons.

⁹³ Par exemple, *HP ships biometric laptop*, CNN.com, 23 juin 2005.

⁹⁴ *Coast to Coast Store Accepts Finger Scan Payments*, Payments News, 19 juin 2006, disponible au www.paymentsnews.com/2006/06/coast_to_coast_.html.

⁹⁵ *Missouri Convenience Stores Introduce Finger Scan Payment Options*. Payments News, 10 août 2006, au www.paymentsnews.com/2006/08/missouri_conven.html.

⁹⁶ Boyle, Matthew. *Let your fingers do the paying*. CNN Money.com, 24 janvier 2006.

⁹⁷ Wolfe, Daniel. *Can Biometric Systems find a Home in the Home?* American Banker online, 6 février 2006.

⁹⁸ *Use fingerprints to withdraw cash from ATMS*, Business Recorder, 15 avril 2006; *Biometrics still out of reach for U.S. ATMs*, CNN.com, 11 octobre 2005.

⁹⁹ *Zions Bank. Zions Bank First Financial Institution to Offer Biometric Check-Cashing Capabilities for Customers, Non-clients*. Communiqué de presse, 5 juillet 2006.

Avant d'examiner plus précisément les qualités ainsi que les lacunes de certaines méthodes d'authentification de nature biométrique, il faut d'emblée décrire un certain nombre de difficultés qu'elles comportent toutes pour nos fins, quoiqu'à des degrés divers.

Premier défi, l'authentification par une technique biométrique requiert qu'on ait d'abord saisi les caractéristiques à vérifier à l'égard de chaque personne susceptible d'utiliser le service auquel est rattaché cette technique. Par exemple et s'il s'agit d'authentifier un consommateur voulant effectuer une opération au guichet automatique, il faudra que l'institution financière ait saisi l'empreinte digitale, palmaire ou rétinienne de chacun de ses clients. Dans le cas des grandes banques canadiennes, on parle de millions de consommateurs.

On conçoit donc d'emblée l'ampleur de la tâche, et les coûts qui en découlent. Il faut d'autre part que la captation de l'information-témoin soit effectuée dans les meilleures circonstances possibles, pour contribuer à la fiabilité du processus, comme on le verra. Il faut donc du personnel compétent, utilisant du matériel de qualité, dans des installations adéquates. L'effort sera considérable. On doit aussi tenir cette banque de données à jour, et donc procéder périodiquement à la captation d'une nouvelle version de l'information-témoin, en raison notamment des modifications que subit le corps en raison d'accidents, de la maladie ou du temps. Il se trouvera par ailleurs toujours des personnes qui, pour une raison ou pour une autre, ne peuvent exhiber la caractéristique biométrique requise conformément aux paramètres du système mis en place. Bref, la constitution des dossiers de vérification et de contrôle constitue un casse-tête étonnamment ardu¹⁰⁰.

Ensuite et lorsqu'on veut procéder à l'authentification, il faut pour capter des mesures biométriques les instruments idoines, utilisés eux aussi dans un contexte approprié. Or le consommateur moyen ne se dotera pas de gaieté de cœur d'un détecteur servant à examiner sa rétine ou la forme de sa main et il pourra même être réticent à installer dans son ordinateur un logiciel servant à mesurer le rythme de ses frappes sur son clavier, par exemple. La quincaillerie – physique ou logique – requise pour la saisie à des fins d'autorisation soulève donc des questions reliées notamment au coût, à la fiabilité et à la popularité: au plan commercial, le succès ne va pas de soi quand il s'agit d'inviter la clientèle à changer notablement ses habitudes.

¹⁰⁰ Entre autres sources, Grüneich, Armin. *Biometrics – hype and reality*. in Economics, Deutsche Bank Research, no. 28, 22 mai 2002. 12 p. Pp. 4-7.

D'autre part, beaucoup de méthodes biométriques fonctionnent d'autant mieux que les mesures sont captées dans un environnement contrôlé, or les domiciles ou les bureaux de millions de consommateurs constituent évidemment et par définition des milieux incontrôlés par les institutions soucieuses d'authentifier des personnes. Cela seul suffirait pour l'instant à écarter l'hypothèse du recours généralisé à la plupart des technologies biométriques dans le cadre des opérations sur l'Internet.

Leur implantation dans d'autres contextes, à titre par exemple de substitut au NIP au guichet automatique ou au point de vente, n'est pas non plus sans poser des défis appréciables. Là encore, il faut envisager les coûts. Il faut aussi pondérer des dimensions aussi pragmatiques que la relation entre l'état d'un lecteur palmaire utilisé en une journée par des centaines de personnes et la protection de la santé publique, par exemple. Même dans ces milieux, les conditions d'utilisation ne seront pas non plus toujours idéales, ce qui peut avoir un effet sur l'exactitude des données saisies, et donc sur la décision d'autoriser ou non le traitement d'une opération.

Ensuite, la fiabilité des méthodes biométriques pose toujours un certain nombre de difficultés. Certains individus ne se conforment pas aux normes: ils ont deux pouces, leur iris se déplace constamment, ils ont été blessés ou une pathologie a modifié leur physiologie... Bref, ils ne peuvent pas être reconnus. Or la logique intrinsèque à ces systèmes fait en sorte que si on abaisse les critères pour reconnaître le plus grand nombre possible de personnes qui devraient l'être, on reconnaîtra aussi erronément des gens qui ne devraient pas l'être – et inversement. Aucune méthode biométrique ne s'est encore montrée infaillible, tant s'en faut.

Quarto, les méthodes biométriques captent des données à la fois «bavardes»¹⁰¹, fluides et «incorrigibles». L'état de l'iris ou de la rétine ou les empreintes digitales peuvent révéler par exemple qu'un individu souffre ou a souffert de problèmes de santé particuliers. D'autre part, la physiologie des personnes change naturellement dans le temps, et il suffit parfois de prendre du poids pour que l'identification par la forme de la main ne fonctionne plus. Il faut donc remettre à jour les banques d'authentification. Par contre et si une identité a été volée, le détenteur légitime d'un identifiant ne peut changer

¹⁰¹ L'utilisation d'authentifiants biométriques pourra par exemple permettre aux commerçants d'affiner leurs programmes de fidélisation en s'assurant qu'un achat donné est bien effectué par le consommateur participant, et non par un tiers auquel il aurait par exemple prêté sa carte: Wolfe, Daniel. *The Tech Scene: Retail Recipe: Combining Biometrics with Loyalty*. American Banker online, 19 octobre 2005.

son empreinte rétinienne aussi facilement qu'il remplacerait un numéro de carte de crédit compromis.

Or des identifiants biométriques peuvent être «empruntés» ou volés. D'abord, on peut par la contrainte obliger un individu à mettre son doigt sur le lecteur d'empreinte digitale¹⁰². Dans certains cas, on peut imiter la donnée biométrique: on a vu par exemple des systèmes de reconnaissance du visage être bernés par une photographie¹⁰³. Surtout et aux fins du traitement informatique, l'identifiant biométrique se trouve tôt ou tard converti en un énoncé binaire qu'il suffit de capter et de réinsérer par la suite dans un système d'identification pour l'abuser¹⁰⁴.

Au plan de la sécurité, le recours à la biométrie pose aussi une difficulté de principe: l'individu n'a à offrir que les empreintes de dix (10) doigts, ou deux (2) iris. Si le recours à la biométrie s'accroît, le consommateur sera donc condamné à utiliser fréquemment le même identifiant, pour des fins totalement différentes. Il s'agira d'une pratique inévitable, mais aussi éminemment imprudente que l'usage d'un même mot de passe pour plusieurs activités distinctes. On pourrait donc, à terme, compromettre globalement la sécurité, au lieu de l'améliorer.

Pour tout compliquer, il existe à l'heure actuelle peu de normes de nature technique ou procédurale en matière d'authentification biométrique et celles qui existent sont inégalement respectées. Chaque fabricant tend donc à offrir un matériel incompatible avec celui de ses concurrents. L'éventuelle mise en réseau de systèmes apparemment similaires, mais pouvant difficilement communiquer entre eux, peut aussi constituer un obstacle important, notamment en matière de mécanismes de paiement¹⁰⁵.

¹⁰² On peut aussi s'embarrasser de moins de difficulté et couper le doigt, tout simplement; certains lecteurs peuvent reconnaître que le doigt est encore bien rattaché à un corps mais, même alors, on ne peut exclure qu'ils puissent être bernés. On assiste ici à un déplacement très pernicieux du risque: on ne perce plus un mur, on vole un doigt pour ouvrir la porte, et non seulement la sécurité se trouve-t-elle de ce fait compromise de toute manière, mais on a aussi porté atteinte à l'intégrité physique d'une personne (et ce même si l'attaque principale, i.e. par exemple l'entrée dans un lieu, échoue de toute manière).

¹⁰³ Les systèmes les plus efficaces (mais aussi les plus coûteux) peuvent toutefois déterminer si ce qu'on présente au détecteur correspond ou non à une personne vivante.

¹⁰⁴ Cela pose évidemment des problèmes pratiques appréciables, mais on ne saurait douter que la chose soit faisable.

¹⁰⁵ On conçoit bien le problème si on imagine que nos banquiers substituent à l'authentification par NIP au guichet automatique celle par empreinte digitale, mais que le capteur d'empreinte du guichet de la Banque de Montréal ne peut techniquement transmettre une information significative au système d'authentification de la Banque de Nouvelle-Écosse, où le consommateur qui désire effectuer une opération à ce guichet détient son compte.

Ce premier tour d'horizon donne déjà un aperçu des écueils qui attendent les banquiers qui voudraient requérir à des modes d'authentification biométriques. Selon la caractéristique particulière à laquelle on veut s'arrêter, l'une ou l'autre de ces difficultés jouera un rôle plus significatif. C'est qu'il y a en effet plusieurs méthodes, dont les qualités et les inconvénients diffèrent.

On met beaucoup l'accent sur les identifiants morphologiques: ils ont trait à la forme d'une partie du corps. Il pourra s'agir de l'empreinte digitale, de l'image de la rétine ou de la cornée, de la forme de la main ou de la forme du visage, par exemple. Les systèmes de reconnaissance de la voix se rangent aussi dans cette catégorie. Ce sont en un sens les identifiants biométriques les plus «naturels», qui correspondent le plus étroitement à la manière dont l'humain reconnaît son semblable. Le système informatique éprouve toutefois beaucoup plus de difficulté à procéder à cette opération que nous effectuons intuitivement.

D'autres identifiants sont plutôt rattachés au comportement de l'individu qu'il s'agit d'autoriser à effectuer une opération. Pour nos fins, la détection des caractéristiques d'utilisation d'un clavier en constitue sans doute l'illustration la plus pertinente, mais on observe aussi des systèmes qui cherchent à reconnaître les caractéristiques d'une signature manuscrite sur un support électronique capable de déceler des éléments comme la vitesse ou le rythme propres à l'autographe d'un individu.

En troisième lieu, la biochimie permet aussi d'identifier une personne et on pourrait par exemple rapprocher l'analyse de l'acide désoxyribonucléique des techniques biométriques. Ces méthodes ne sont toutefois pas du tout pratiques¹⁰⁶ à des fins d'authentification courantes dans le cours d'opérations de consommation et on ne les abordera donc pas.

On s'attardera ici surtout aux identifiants morphologiques, et notamment à la dactyloscopie, à la lecture de l'iris et à l'analyse faciale. Ces trois cas de figure permettront d'illustrer plus précisément la plupart des difficultés que peut entraîner le recours à des modes d'authentification biométriques.

B- Une recension partielle

¹⁰⁶ En raison notamment du coût, du temps requis pour procéder à une analyse et des questions particulièrement sérieuses qu'elles soulèvent en matière de gestion des renseignements personnels.

1- les identifiants biométriques morphologiques

Les données morphologiques constituent de loin le type d'identifiant biométrique le plus usité. De nombreuses entreprises tentent de se tailler leur part dans un marché qu'elles cherchent à gonfler en multipliant les promesses à l'égard des performances de leurs systèmes. Les événements de septembre 2001 ont évidemment créé un contexte qui leur paraît propice à cet égard.

Le recours aux données morphologiques recèle toutefois de nombreux pièges. Il peut s'avérer coûteux pour les entreprises. La fiabilité des technologies n'est pas toujours avérée, ce qui incommode tant les commerçants que les consommateurs. Elles requièrent aussi, à des degrés variables, une intrusion dans la sphère d'autonomie personnelle des consommateurs qui peut leur déplaire significativement. Un examen sommaire des principales techniques utilisant ces données permet de mieux le comprendre.

a) la dactyloscopie

i) des empreintes confuses?

Le recours aux empreintes digitales demeure le mode d'identification biométrique le plus utilisé dans le monde, non seulement à des fins policières mais aussi dans d'autres contextes. On le connaît si bien que la technique ne requiert qu'une brève explication: en principe, entend-on depuis des décennies, deux êtres humains ne pourraient avoir des empreintes identiques, de sorte qu'elles peuvent servir à distinguer des individus. Les variantes ont trait à la structure générale de l'empreinte mais aussi à ce que les experts qualifient de «minuties», i.e. les détails des volutes des empreintes.

Il paraît cependant acquis qu'il n'existe aucune étude scientifique quantifiant avec quelque certitude la probabilité que les empreintes de deux personnes différentes soient identiques ou, du moins, si similaires qu'on présumera qu'elles proviennent de la même personne¹⁰⁷.

L'empreinte humaine normale compte de soixante-quinze (75) à cent soixante-quinze (175) minuties¹⁰⁸. Il n'y a pas de consensus dans la communauté internationale des analystes d'empreintes digitales quant au nombre de minuties identiques qu'on doit

¹⁰⁷ Epstein, Robert. *Fingerprints meet Daubert: the myth of fingerprint "science" is revealed*. [2001-2] 75 Southern California Law Review 605.

¹⁰⁸ *Ibid.*, p. 608, citant un document émanant du *Federal Bureau of Investigation*.

observer pour conclure à l'identité de deux empreintes différentes¹⁰⁹, mais les autorités policières de certains États européens fixent par exemple ce nombre à seize (16)¹¹⁰. Or il se produit que les empreintes de deux personnes différentes soient assez similaires:

«It has been well documented that fingerprints from different people can share a limited number of ridge characteristics in common. Israeli fingerprint examiners, for instance, have found fingerprints from two different people that contain seven matching characteristics. As these examiners candidly acknowledge, “an expert with many years of experience behind him” could make a false identification when comparing two such prints. No scientific study has been performed that reasonably indicates the probabilities of fingerprints from different people having varying numbers of matching ridge characteristics».¹¹¹

L'affaire Mayfield a démontré clairement les difficultés que pose l'interprétation d'empreintes digitales en 2005. On se souvient bien sûr des attentats de Madrid, le 11 mars 2004. Les autorités espagnoles ont prélevé sur un sac de détonateurs liés à ces attentats un certain nombre d'empreintes digitales latentes et incomplètes et, par l'entremise d'Interpol, ont prié le *Federal Bureau of Investigation* des États-Unis (ci-après le «FBI») de déterminer si ces empreintes étaient fichées dans les dossiers des autorités états-uniennes¹¹².

Le personnel spécialisé du FBI a cru constater la présence de dix (10) minuties identiques entre l'empreinte recueillie par les autorités espagnoles, d'une part, et une empreinte associée à Brandon Mayfield, un citoyen des États-Unis et avocat habitant en Oregon. Dès ce constat, M. Mayfield a fait l'objet d'une enquête serrée, qui a notamment permis d'établir qu'il est musulman, marié à une femme d'origine égyptienne et qu'il a

¹⁰⁹ *Ibid.*, p. 610.

¹¹⁰ *Ibid.*, p. 636.

¹¹¹ *Ibid.*, pp. 610-1 (notes infrapaginales omises).

¹¹² U.S. Department of Justice. Office of the Inspector General. *A Review of the FBI's Handling of the Brandon Mayfield Case – Unclassified Executive Summary*. Washington, Office of the Inspector General Oversight and Review Division, janvier 2006. 20 p. P. 1.

déjà représenté en justice une personne condamnée pour terrorisme. M. Mayfield a été arrêté le 6 mai 2004 et mis en détention préventive¹¹³.

Le 13 avril, le FBI avait cependant été informé que les autorités espagnoles concluaient quant à elles que les empreintes rattachées au crime et celles de M. Mayfield ne concordait pas. Le 19 mai, les autorités espagnoles ont annoncé que les empreintes rattachées au crime étaient en fait celles d'un citoyen algérien, M. Ouhnane Daoud. Le FBI a retiré ses conclusions quant à l'appartenance des empreintes le 24 mai et M. Mayfield a été remis en liberté¹¹⁴.

L'affaire Mayfield illustre trois choses. D'une part, des individus qui n'ont aucun lien l'un avec l'autre peuvent avoir des empreintes digitales qui paraissent, au moins dans certaines circonstances, très similaires. Ensuite, le nombre d'éléments similaires jugé suffisant dans la communauté des analystes d'empreintes digitales pour associer une empreinte à un nom est remarquablement peu élevé. *Tertio*, les circonstances dans lesquelles des empreintes sont prélevées pour analyse et le contexte dans lequel elles sont analysées peuvent contribuer à l'atteinte de conclusions erronées.

Comme l'indique Epstein, en effet, l'apparence d'une empreinte peut être modifiée par plusieurs éléments:

«All prints, both inked and latent, are subject to various types of distortions and artifacts. The most common is pressure distortion, which occurs when the print is being deposited. Other types of distortion can be caused by the shape of the surface on which the print has been deposited and by the media used to develop and lift the print. Significantly, distortion can cause a ridge characteristic to appear as something other than what really is.»¹¹⁵

Même deux empreintes d'un même doigt prises dans des conditions idéales ne seront pas identiques, en raison de cette distorsion physique¹¹⁶.

¹¹³ *Ibid.*, pp. 2-3, 6-7.

¹¹⁴ *Ibid.*, pp. 2-3.

¹¹⁵ Epstein, *op. cit.*, p. 609.

¹¹⁶ *Ibid.*, p. 631.

On voit donc clairement les difficultés que pose le recours à la dactyloscopie à des fins d'authentification. Il faut d'abord prélever, dans les meilleures conditions possibles, une ou plusieurs empreintes de la personne qui voudra ultérieurement être autorisée à effectuer une opération. Le nombre d'empreintes utilisées joue en effet sur la qualité des résultats du processus d'authentification.

Une étude sommaire menée dans le contexte de l'implantation d'un processus généralisé d'identification dactyloscopique aux fins de l'administration du régime de sécurité sociale dans la république des Philippines a permis d'établir que, compte tenu de la qualité de la performance des procédés commerciaux de dactyloscopie, on ne pouvait atteindre à des niveaux de fiabilité acceptables qu'en comparant les empreintes de deux (2) doigts d'un individu avec le contenu de la banque de données¹¹⁷. La comparaison des empreintes d'un seul doigt donnait en effet ce résultat que dans un cas sur dix (10), on faisait défaut d'identifier effectivement la personne en cause. En comparant les empreintes de deux (2) doigts du sujet, ce taux de faux rejet tombait à environ un pour cent (1%) – ce qui demeure quand même assez considérable. Le taux de fausses acceptations se trouvait quant à lui dans l'ordre du cas sur un million: les systèmes testés détectaient donc bien les inconnus, mais omettaient assez souvent de reconnaître des individus qu'ils auraient dû identifier. Même en admettant que les technologies se sont améliorées dans la dernière décennie – et on y revient, la marge d'erreur demeure donc élevée.

ii) des défis pratiques

La saisie et le traitement de ces données peuvent par ailleurs donner lieu à des erreurs administratives. Par exemple et dans le cadre de l'application du régime de dactyloscopie des visiteurs aux États-Unis, on a recensé des cas où on a confondu par exemple dans le dossier d'une personne l'index droit et l'index gauche, de sorte que cet individu fait l'objet d'un contrôle en règle chaque fois qu'il franchit les frontières états-uniennes¹¹⁸.

La constitution d'une telle banque de données pose par ailleurs des risques manifestes au plan de la sécurité: il peut s'agir d'une cible tentante pour des criminels tout

¹¹⁷ Wayman, James L. *The Philippine AFIS Benchmark Test Results*. slnd. Ce sommaire des résultats d'une étude d'implantation de technologies concurrentes, réalisée en mai 1997, porte sur un échantillon de quelques centaines de volontaires. On le trouvera sur le web au www.dss.state.ct.us/digital/ditutor/bhsugijlw.htm.

¹¹⁸ *Some visitors delayed by mismatched fingerprints on passports*, CNN.com, 23 juin 2005.

comme d'ailleurs, dans certains contextes et dans ces cas avec un mandat de perquisition, pour les forces de l'ordre¹¹⁹. Il y a aussi risque notable de détournement de finalité.

S'ajoute évidemment la problématique du processus de constitution de la banque de données de contrôle: pour une institution financière, il s'agirait d'obtenir une ou plusieurs empreintes digitales de chacun de ses clients, dans des conditions aussi idéales que faire se peut. Si les processus dactyloscopiques partagent ces problèmes avec les autres méthodes biométriques, il n'est pas sans intérêt de noter que la cour suprême de Taiwan a émis en juin 2005 une injonction interlocutoire pour bloquer la saisie des empreintes digitales dans le cadre d'un processus de création d'une carte d'identité nationale, en soulignant notamment qu'il s'agissait d'une opération extrêmement coûteuse et que ces fonds publics auraient été gaspillés si les tribunaux devaient conclure sur le fond que ce programme est en tout ou en partie inconstitutionnel¹²⁰.

Une fois qu'on a stocké les empreintes de la clientèle, il faut prélever ponctuellement l'empreinte de l'individu qui veut bénéficier d'une autorisation pour effectuer une opération. On ne peut évidemment pas, dans un contexte de nature commerciale, prélever l'empreinte comme le font les autorités policières, avec un tampon encreur. On utilise donc un lecteur optique ou électronique. Les technologies varient considérablement, tout comme leur efficacité. Une étude récente recense sept (7) technologies distinctes en matière de *solid-state fingerprint scanner technologies*, par exemple¹²¹.

Ces lecteurs dactyloscopiques peuvent être classés en deux grandes catégories: certains requièrent l'utilisateur de glisser son doigt le long d'une étroite rangée de senseurs, tandis que d'autres, plus coûteux, sont sensiblement de la taille d'une empreinte et il suffit d'y déposer le doigt. Les premiers réassemblent numériquement les éléments d'image prélevés, ce qui peut notamment induire des erreurs dues à la manière dont le doigt a été glissé le long des senseurs (et notamment à la vitesse utilisée)¹²², ou

¹¹⁹ même si on sait que dans la quasi-totalité des cas, on stocke non pas une image exacte de l'empreinte, mais une dérivation mathématique effectuée à partir de l'image, cette dernière étant ensuite effacée.

¹²⁰ *Taiwan Constitutional Court places fingerprinting plan on hold*. Privacy International, 22 juin 2005. À l'opposé, le cabinet japonais a pour sa part approuvé récemment un programme de dactyloscopie des visiteurs: Associated Press. *Japanese Cabinet approves plan to fingerprint visitors*. Gulfnews.com, 8 mars 2006, au www.gulfnews.com/world/Japan/10023910.html.

¹²¹ Wasserman, Philip. *Solid-State Fingerprint Scanners: A Survey of Technologies*. Gaithersburg (MD), National Institute of Standards and Technologies, décembre 2005. Présentation *Powerpoint* disponible au www.itl.nist.gov/iaui/894.03/pact/SSFS_113005.pdf.

¹²² *Ibid.*

potentiellement, à l'efficacité des logiciels utilisés pour recomposer l'image. Ces lecteurs sont notamment utilisés pour certains ordinateurs portables et peuvent l'être pour des téléphones mobiles, par exemple.

D'autre part, aucun des senseurs de plus grande surface qui sont actuellement commercialement disponibles ne correspondrait aux normes états-uniennes pertinentes relatives à la qualité de l'image¹²³. Tous les senseurs présentement disponibles dans le marché permettraient par ailleurs la captation des images d'un seul doigt, et non de plusieurs.¹²⁴

Des tests menés par un groupe en République fédérale d'Allemagne en 2002 ont quant à eux indiqué que beaucoup de senseurs disponibles dans le marché à l'époque étaient terriblement vulnérables. Par exemple, l'apposition d'un doigt sur le senseur laisse le plus souvent une empreinte latente; dans le cas de certains senseurs, il a suffi de réchauffer un peu l'air au-dessus du senseur en exhalant pour que l'appareil relise l'empreinte latente et croie par conséquent qu'on adressait une demande d'authentification avec cette empreinte laissée par une personne alors absente¹²⁵. On imagine l'effet dans un réseau de guichets automatiques...

S'ajoutent évidemment à ces problèmes techniques les aléas de la vie courante, qui peuvent faire en sorte qu'on a par exemple une cicatrice au doigt précisément là où se trouve une minutie déterminante de l'empreinte, ou un pansement adhésif qui recouvre la plus grande portion de l'empreinte, ou qu'on n'a pas eu l'occasion d'utiliser un produit détachant pour éliminer quelques gouttelettes de peinture qui s'avèreraient elles aussi déplorablement mal situées.

En fait, on constate empiriquement qu'une proportion de deux (2%) à cinq pour cent (5%) de la population d'un pays comme les États-Unis ne peut fournir une empreinte digitale fiable, en raison par exemple des dommages causés par l'âge, par du travail manuel intensif ou l'exposition professionnelle prolongée à des produits corrosifs. Qui plus est, les empreintes des personnes provenant de certaines régions d'Asie seraient nettement plus difficiles à saisir que la moyenne¹²⁶ et on conçoit sans peine les problèmes

¹²³ *Ibid.*

¹²⁴ *Ibid.*

¹²⁵ Thalheim, Lisa; Krissler, Jan; Ziegler, Peter-Michael. *Body Check – Biometric Access Protection Devices and their Programs Put to the Test*. mai 2002. Consulté au www.heise.de/ct/english/02/11/114/.

¹²⁶ United States. General Accounting Office. *Using Biometrics for Border Security*. Washington, novembre 2002. Disponible au www.gao.gov/new.items/d03174.pdf.

juridiques en matière de discrimination systémique ou de gestion de renseignements personnels de nature «sensible» qui peuvent découler de ce dernier type de préoccupation.

Pragmatiquement, il sera également utile que la surface du capteur soit nettoyée régulièrement, pour assurer la qualité de l'image (et quel impact auraient des égratignures sur cette surface?). On pense ici par exemple à des équipements publics comme des guichets automatiques, pour lesquels cette préoccupation – et celle liée à l'hygiène – s'impose davantage qu'à l'égard de l'authentification d'une opération réalisée avec l'ordinateur personnel d'un consommateur. Dans ces deux types de cas cependant, la question de l'usage frauduleux d'une empreinte latente soulève des problèmes réels.

iii) des résultats insatisfaisants

La fiabilité des images captées à des fins d'authentification paraît donc, dans l'état actuel du marché, moins qu'absolue. Cela aura inévitablement un effet sur le processus de comparaison entre l'image captée, d'une part, et l'image stockée, d'autre part. Cependant et même si on fait abstraction de cet élément, la comparaison informatisée d'images dactyloscopiques à des fins d'authentification ou d'identification ne donne pas des résultats parfaits. Une étude publiée en 2005 indique en effet que les taux d'erreur vont, à l'égard des systèmes testés, d'environ un pour cent (1%) à près de quarante-quatre pour cent (43,9%) dans un cas extrême. Sur dix-neuf (19) systèmes testés, onze (11) avaient des taux d'erreur de moins de cinq pour cent (5%)¹²⁷.

Plus précisément,

«NIST has conducted testing of one-to-one SDK (Software Development Kit) based COTS (Commercial Off-the-Shelf) fingerprint matching systems to evaluate the accuracy of one-to-one matching used in the US-VISIT program. Fingerprint matching systems from eleven vendors not used in US-VISIT were also evaluated to insure that the accuracy of the matcher tested was comparable to the

¹²⁷ Watson, Craig; Wilson, Charles; Marshall, Karen; Indovina, Mike; Snelick, Rob. *Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers*. Publication NISTIR 7221. sl, National Institute of Standards and Technology, 22 avril 2005. 17 p. Disponible au www.fingerprint.nist.gov/SDK/ir_7221.pdf.

most accurate available COTS products. The SDK based matching application was tested on 20 different single finger data sets of varying difficulty. The average true accept rate (TAR) at a false accept rate of 0.01% was better than 98% for the two most accurate systems while the worst TAR at a FAR or 0.01% was greater than 94%.»¹²⁸

D'abord, il s'agissait donc d'un test centré sur la comparaison de données, et non de la simulation d'une situation réelle où certaines des données comparées sont captées en situation non contrôlée.

Comme on l'a noté *supra*, la comparaison de données biométriques requiert toujours un compromis. Plus on exige de certitude pour éviter de donner une autorisation à qui ne devrait pas la recevoir, plus on augmente la proportion de gens qui devraient être autorisés mais qui ne le seront pas parce que l'authentifiant qu'ils présentent est jugé hors-norme. C'est ce que traduisent les données qu'on trouve à la fin de la citation précédente: quand on fixe les paramètres d'évaluation de manière à exclure 99,99% de ceux qui doivent être exclus (soit le «FAR»), le taux d'exclusion de ceux qui devraient être admis va de un (1%) à cinq pour cent (5%) dans la plupart des cas.

Transposons des résultats de cette nature dans un contexte bancaire et présumons par exemple qu'on substitue la captation d'une empreinte dactyloscopique à la composition du numéro d'identification personnel afin d'effectuer des retraits de numéraire au guichet automatique. Dans un cas sur dix mille (10 000), un fraudeur parviendra à effectuer un retrait parce que le processus d'analyse conclura erronément qu'il est bien la personne autorisée à faire l'opération demandée. Par contre et dans au moins un cas sur cent (1%), le véritable client se verra refuser la possibilité de retirer des fonds parce que le système conclura à tort qu'il n'est pas lui-même. Si on présume que le consommateur moyen fait maintenant deux (2) opérations au guichet par semaine¹²⁹, soit une centaine par année, il souffrirait en moyenne une fois l'an un refus d'accès à son compte parce qu'on ne reconnaîtrait pas son empreinte. Pour les institutions financières et compte tenu de la quantité d'opérations encore réalisées au guichet automatique, il

¹²⁸ *Ibid.*, p. 2.

¹²⁹ La fréquence moyenne était de 7,6 opérations au guichet par mois au Québec en 1998: CROP, *op. cit.*, Q 23 b), et il est plus que vraisemblable que cette fréquence ait augmenté depuis.

s'agirait là assez vite d'un cauchemar administratif et réputationnel: le secteur financier ne peut vraiment se permettre des marges d'erreur de cette ampleur.

Comme le note une firme d'experts,

«With tens of millions of payment transactions done daily, hundreds of thousands of improperly denied transactions (or in ToweGroup's terms, "insults") would take place through the ubiquitous use of fingerprint-reading verifications [...]»¹³⁰

Un tel taux de refus paraît inacceptablement élevé, mais c'est pourtant celui que produirait le meilleur système testé dans le cadre de cette étude, et sans tenir compte des difficultés de captation de l'empreinte dans le contexte pratique d'un lecteur adjacent à un guichet automatique dans un lieu public fréquenté et où les conditions de saisie des données peuvent varier notablement.

Par conséquent et même s'il s'agit sans doute du processus biométrique le plus connu et de l'un des plus faciles en principe à déployer, on peut croire que les institutions financières canadiennes, si elles procèdent à une analyse de risque rigoureuse, conclueront qu'elles ont fort peu à gagner, et beaucoup à perdre, à recourir à l'authentification dactyloscopique en matière d'opération de paiement des consommateurs¹³¹.

b) l'observation de l'iris

L'iris est un muscle circulaire, situé derrière la cornée de l'oeil, et qui règle la quantité de lumière entrant dans cet organe. À l'observation, on peut constater la présence de ligaments, mais aussi dans sa structure des sillons, des arêtes, des anneaux et une collerette¹³². Chaque iris serait donc foncièrement différent: même les deux iris d'une personne ne sont pas identiques¹³³. Par ailleurs et compte tenu de son emplacement dans le corps humain, l'iris serait en général peu susceptible d'altérations¹³⁴ et son observation

¹³⁰ Fest, Glen. *Cards: Biometrics Stalled Amid the Hype*. Bank Technology News, août 2005, au www.banktechnews.com/article.html?id=20050729VXE0TOO4.

¹³¹ D'autres types d'activité, comme l'identification à l'embauche ou l'authentification du personnel affecté à des zones à haute sécurité, peuvent commander une analyse différente.

¹³² Daugman, John. *How Iris Recognition Works*. Cambridge, sd. 10 p. Disponible au www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf. Le Pr Daugman s'est spécialisé dans les questions reliées à l'identification par l'iris et détient plusieurs brevets dans ce domaine.

¹³³ *Ibid.*, pp. 5-6.

¹³⁴ *Ibid.*, p. 1.

ne permettrait pas de déceler beaucoup de données relatives à la santé de l'individu en cause.

L'iris constituerait donc à première vue un identifiant pratiquement parfait, d'autant que son aspect plat le rend assez peu susceptible aux variations d'éclairage au moment de l'examen¹³⁵, qui s'effectue par l'envoi dans l'oeil d'un rayon électromagnétique dont la fréquence est près de l'infra-rouge, et qui est donc imperceptible pour l'humain¹³⁶. Les logiciels de comparaison des images d'iris actuellement utilisés permettraient d'effectuer jusqu'à cent mille (100 000) vérifications à la seconde, de sorte qu'il suffit de mettre en série un certain nombre d'ordinateurs de modèle courant pour traiter rapidement des volumes considérables¹³⁷ et authentifier une opération en quelques secondes.

Selon le même chercheur, qui a examiné les résultats obtenus dans le cadre du programme de contrôle de l'immigration des Émirats arabes unis, le mécanisme de reconnaissance de l'iris permet d'obtenir des résultats remarquables. L'auteur décrit ce programme dans les termes suivants:

«In the summer of 2001 the UAE Ministry of Interior launched a national border-crossing security programme that is today deployed at all 17 of the UAE's air, land and sea ports. It is based upon mathematical analysis of the random patterns visible in the iris of a person's eye (*iris recognition*), using algorithms developed by the author of this report [...]»¹³⁸

L'ampleur du programme de reconnaissance de l'iris déployé par les Émirats ne manque pas d'étonner: des informations relatives à plus de neuf cent mille (900 000) iris (et donc autant de personnes) dans la banque de données, mille (1 000) nouveaux dossiers par jour¹³⁹, neuf mille (9 000) personnes authentifiées chaque jour lorsqu'elles traversent la

¹³⁵ *Ibid.*

¹³⁶ *Ibid.*, p. 2.

¹³⁷ *Ibid.*, p. 4.

¹³⁸ Daugman, John. *The United Arab Emirates iris study: Results from 200 billion iris cross-comparisons*. Cambridge, août 2005. 14 p. Disponible au www.adpolice.gov.ae/PDF/UAEREport.pdf. Ci-après «Daugman 2005».

¹³⁹ notamment des personnes emprisonnées ou détenues dans des centres de déportation.

frontière par une procédure durant en moyenne deux (2) secondes¹⁴⁰ et une moyenne de cent vingt-six (126) tentatives d'entrée non autorisée au pays détectées chaque jour, pour plus de soixante-deux mille (62 000) personnes à qui on a interdit l'entrée au pays depuis la mise en oeuvre du programme¹⁴¹. Il s'agirait de la plus importante banque de données relatives à la reconnaissance de l'iris au monde.

Au moment où le Pr Daugman a évalué l'efficacité du système déployé aux Émirats, la banque de données contenait un peu plus de six cent mille (632 500) dossiers, rattachés à des individus de plus de cent nationalités différentes. Ce nombre de dossiers a permis de procéder à des comparaisons entre deux cent milliards (200 G) de paires d'iris. Selon le chercheur, on n'aurait détecté aucun cas d'identité entre les iris de deux personnes différentes¹⁴².

La méthode de reconnaissance par l'iris n'est pas parfaite pour autant. D'abord, les paupières et les cils, notamment, constituent des obstacles à l'observation et leur effet doit être compensé¹⁴³. Des caméras de modèles différents fournissent des images de qualité et de résolution variables, selon la nature de leurs composantes optiques et la fréquence particulière du rayon envoyé vers l'iris¹⁴⁴. Compte tenu que l'iris est relativement plat, les variations de facteurs comme l'éclairage ou la distance à la caméra relatives à la saisie originale d'une image ou à la captation ultérieure à des fins d'authentification n'auraient pas d'effets catastrophiques sur la capacité d'authentification¹⁴⁵. Les autorités des Émirats arabes unis appliquent néanmoins des règles assez strictes au plan de la captation des images, pour limiter toute variation induite¹⁴⁶.

Les personnes interdites de séjour qui souhaitent néanmoins entrer aux Émirats avaient par ailleurs découvert un subterfuge: certaines gouttes médicinales dilatent l'iris, ce qui leur permettait de ne pas être identifiées¹⁴⁷. Les logiciels de comparaison des images ont été modifiés pour tenir compte de ces paramètres et les garde-frontières... gardent l'oeil ouvert pour déceler les individus à l'oeil anormalement dilaté.

¹⁴⁰ Hilotin, Jay. *Deportees caught with eyes wide open*. Gulfnews.com, 2 avril 2006.

¹⁴¹ Salama, Samir. *Iris scanner blocks 62,000 illegals*. Gulfnews.com, 3 mai 2006.

¹⁴² Daugman 2005, pp. 3, 6-7.

¹⁴³ *Ibid.*, p. 4. Des problématiques culturelles comme le port de la burkha doivent aussi être prises en compte.

¹⁴⁴ *Ibid.*, pp. 7-8.

¹⁴⁵ Daugman, pp. 8-9.

¹⁴⁶ Daugman 2005, p. 7.

¹⁴⁷ Hilotin, Jay. *Deportees caught with eyes wide open*. Gulfnews.com, 2 avril 2006.

Bien entendu, les personnes dont les yeux ont subi des dommages anatomiques éprouvent de sérieuses difficultés avec cette méthode. En particulier, les gens ayant souffert de cataractes ou de glaucôme peuvent être inadmissibles¹⁴⁸. D'autres¹⁴⁹ souffrent d'un problème de santé comme le nystagmus, qui fait que leur iris est constamment en mouvement, et ne peuvent donc faire l'objet d'une authentification, à moins qu'on recoure à des caméras très perfectionnées mais, bien sûr, nettement plus coûteuses. Les personnes dont la vue est basse, mais dont l'iris peut cependant être observé, éprouvent d'autre part fréquemment de la difficulté à bien placer leur œil pour que l'image de leur iris soit captée, les indicateurs à cet égard étant évidemment d'ordre visuel¹⁵⁰.

Il semblerait d'autre part qu'un certain nombre au moins d'études visant à établir la fiabilité de l'observation de l'iris seraient moins convaincantes qu'elles ne le semblent parce qu'on aurait exclu de l'échantillon testé ces personnes qui ne peuvent donner de bons résultats¹⁵¹. Cette tranche exclue pourrait atteindre jusqu'à deux pour cent (2%) de l'ensemble de la population¹⁵². L'usage de verres de contact rigides ferait aussi obstacle à la méthode¹⁵³.

Plus génériquement, on a dans le passé publié des enquêtes ou des études révélant qu'on avait pu tromper des systèmes de reconnaissance de l'iris en utilisant des lentilles cornéennes ou, tout simplement, en présentant au lecteur une photo d'un œil inscrit dans la banque de données¹⁵⁴. On peut aussi envisager la contrefaçon en utilisant une image vidéo (ou une image sur un téléphone mobile), l'extraction de l'œil¹⁵⁵, ou la contrainte exercée contre l'individu dont l'iris peut servir d'authentifiant. Certains systèmes de reconnaissance sont assez perfectionnés pour éviter d'être ainsi trompés, mais ils ne l'ont assurément pas tous été dans le passé¹⁵⁶. Les méthodes permettant d'assurer que l'«iris»

¹⁴⁸ *The Identity Project – an assessment of the UK Identity Cards Bill and its implications*. Londres, London School of Economics, 27 juin 2005. 283 p. (Ci-après «LSE»). Pp. 177-179.

¹⁴⁹ dont le directeur de *Privacy International*.

¹⁵⁰ LSE, *loc. cit.*

¹⁵¹ *Ibid.*, p. 177.

¹⁵² *Ibid.*, p. 179, citant la firme Iridian Technologies, spécialisée dans ce domaine.

¹⁵³ *Ibid.*, p. 181.

¹⁵⁴ Toth, Bori. *Liveness Detection for Iris Recognition*. sl, Deloitte & Touche, mars 2005. Présentation Powerpoint au *NIST Workshop on Biometrics and E-Authentication over Open Networks*.

¹⁵⁵ Les amateurs de l'auteur Dan Brown songeront à cet égard aux premiers chapitres du roman *Anges et démons*.

¹⁵⁶ Toth, *op. cit.*

examiné est bien réel, et rattaché à un être vivant, sont souvent d'autant plus efficaces que la caméra utilisée pour l'authentification est proche de l'oeil examiné¹⁵⁷.

Au total, il semble que l'iris puisse constituer un authentifiant plus précis que l'empreinte digitale. Malgré l'ampleur du programme des Émirats arabes unis, on est toutefois encore loin d'une démonstration à très grande échelle de la faisabilité pratique d'un processus d'authentification par l'iris des opérations de paiement électronique effectuées par les consommateurs canadiens. En particulier, la saisie de l'image à valider pour autoriser une opération donnée risque de susciter des difficultés: même en milieu relativement contrôlable, comme au guichet automatique, certaines personnes seraient inévitablement exclues tandis qu'en milieu privé, comme lorsqu'un consommateur veut effectuer un paiement sur l'Internet, l'individu devrait s'être muni d'un appareil de type photographique idoine et, à moins qu'on déploie des systèmes très sophistiqués, le risque de fraude par la présentation d'une image, par exemple, pourrait demeurer appréciable.

Là encore, on voit donc mal pourquoi, à la réflexion, les institutions financières canadiennes devraient se lancer dans une telle aventure.

c) la comparaison faciale

Parce qu'il n'y a rien de plus naturel pour un humain que d'en reconnaître un autre par ses traits, on pourrait croire que la méthode biométrique la plus simple viserait l'authentification par la morphologie du visage. On constate au contraire qu'il s'agit d'un défi colossal.

Dans le cadre d'une image, par exemple, un logiciel de reconnaissance doit d'abord identifier le visage, tenir compte de sa position et de sa grosseur dans l'image, prendre en compte son orientation... Bien entendu, le voile, par exemple, vient compliquer l'examen. En somme et dès qu'il s'agit de comparer des images qui ne sont pas prises dans des environnements extrêmement contrôlés, les facteurs d'erreur se multiplient.

La reconnaissance du visage opère le plus souvent par la comparaison de certains paramètres particuliers, comme la distance entre les yeux ou les oreilles¹⁵⁸, de sorte que des subterfuges comme la variation de la capillarité ou le port de lunettes ne devraient pas avoir d'effets sur les résultats. Par contre, des personnes au teint très pâle ou albinos sont pratiquement invisibles pour les logiciels qui mesurent ces distances, parce qu'elles se

¹⁵⁷ *Ibid.*, p. 9.

¹⁵⁸ On ne peut cependant pas exclure que ces données puissent comporter implicitement des indications sur l'origine ethnique des personnes.

confondent le plus souvent pour la caméra avec le fond blanc généralement utilisé dans un environnement contrôlé.

En somme, on ne dispose encore d'aucune garantie que ces systèmes soient plus performants que les modes d'identification dactyloscopiques ou iridiens.

2- les autres identifiants biométriques

La manière dont une personne tape sur un clavier lui serait propre et pourrait faire office d'authentifiant. Cette technique comporte évidemment l'avantage qu'elle est pratiquement transparente: dans bien des cas, comme la réalisation d'une opération sur l'Internet, le consommateur utilise de toute manière un clavier qu'il a déjà. Cette méthode est déjà commercialisée¹⁵⁹ et fait également l'objet de recherches.

Elle comporte cependant des inconvénients. Tous les claviers ne sont en effet pas identiques, et ils varient notamment en vertu de la langue. La personne dont les caractéristiques sont déjà connues d'un système d'authentification et qui utilise tout à coup un clavier qui ne lui est pas familier verra son rythme modifié, et ne pourra donc être identifiée. La difficulté peut être particulièrement importante pour les gens qui se déplacent fréquemment à l'étranger. et qui veulent avoir accès à distance au système informatique de leur entreprise, par exemple. Il est également possible que le rythme d'une personne puisse être observé et imité. La personne qui souffre d'une blessure légère à un doigt ou une main modifiera sans doute aussi son rythme, et pourrait ne pas être reconnue comme étant elle-même.

L'intérêt que peut susciter cette technologie est également atténué par cette difficulté qu'il ne paraît pas exister d'évaluation indépendante de son efficacité.

Quant aux mécanismes de reconnaissance de la voix, ils comportent cette première – et très grave – difficulté qu'ils peuvent assez facilement être trompés par un enregistrement de bonne qualité. On devrait aussi prendre en compte ce détail que la voix constitue un révélateur étonnamment puissant d'éléments comme l'état émotionnel d'une personne¹⁶⁰: la captation d'un échantillon de contrôle pourrait donc poser des problèmes à l'égard de la nature des renseignements personnels obtenus, et la comparaison pourrait dans certains cas s'avérer difficile dans le temps.

¹⁵⁹ On consultera par exemple le www.biopassword.com.

¹⁶⁰ *Bored on the phone? Beware the Jerk-O-Meter*. CNN.com, 12 août 2005.

V- La question de l'architecture

The problems that exist in the world today cannot be solved by the level of thinking that invented them.

Albert Einstein

A- Un problème systémique

Cette citation d'Einstein, qui n'est pas sans rappeler le théorème de Gödel¹⁶¹, comporte bien sûr quelque chose d'un rien déprimant en matière de sécurité et, notamment, d'authentification. Le défi de construire des systèmes sécuritaires, fiables et commodes à un prix abordable paraît considérable, d'autant que les architectes qui le tentent font face à une autre triste réalité: il est en général beaucoup plus facile d'attaquer que de concevoir et de vérifier. L'offensive comporte souvent peu de risque et peut rapporter beaucoup, alors que la prévention de toutes les attaques concevables constitue une tâche pratiquement insurmontable. En somme, l'attaquant qui veut percer un système n'a qu'à réussir une fois, tandis que le défenseur doit réussir à contrer toutes les attaques.

Or les systèmes, notamment dans les domaines de la télématique et de l'informatique, deviennent de plus en plus complexes, et peuvent donc devenir de plus en plus fragiles. À la limite, la proportion d'architectes ou d'ingénieurs vraiment compétents par rapport au nombre croissant de problèmes complexes tend à diminuer: le travail défensif s'alourdit plus rapidement qu'on peut recruter des soldats.

La diversité des attaques possibles, que n'entrevoit pas le néophyte, stupéfie¹⁶². Le risque juridique relativement faible que courent les fabricants de produits et services de sécurité même en cas de défaillance de leur matériel fait en sorte qu'ils voient peu de raison à consacrer des efforts considérables à assurer la robustesse de leurs systèmes, et beaucoup à en faire la promotion.

¹⁶¹ Pour mémoire, Gödel a irréfutablement démontré il y a quelques décennies qu'il existe dans tout système logique au moins un axiome, i.e. un énoncé formellement indémontrable selon les règles de ce système.

¹⁶² On lira par exemple une présentation PowerPoint de 2002: Kocher, Paul. *Illusions of Security*. 11th USENIX Security Workshop, 8 août 2002, au www.usenix.org/events/sec02/Kocher.pdf. Si les détails technologiques ont pu évoluer quelque peu depuis, l'essentiel de l'analyse demeure tout à fait juste.

Il en résulte des défaillances parfois monstrueuses. Au Royaume-Uni, on avait remplacé dans une prison, au coût de trois millions de livres sterling (3 M £), les serrures traditionnelles par des lecteurs d'empreintes digitales. Il a fallu peu de temps pour que les détenus trouvent le moyen de déverrouiller les portes aussi facilement que le faisaient les gardiens, de sorte qu'on a dû revenir au trousseau de clés traditionnel¹⁶³. Toujours en Grande-Bretagne, l'industrie bancaire a constaté récemment qu'elle a eu tort d'utiliser une technologie d'autorisation hors ligne, et non en ligne, pour des opérations effectuées avec une carte à puce: il en résulte une vulnérabilité sérieuse pour le système qui découle d'un choix qui paraît inexplicable en principe, mais qui s'explique quand on sait que la technologie hors ligne est nettement moins coûteuse que la technologie en ligne¹⁶⁴.

Hors du cadre de la biométrie mais dans le secteur financier, on a constaté en 2005 que les guichets automatiques d'une bonne moitié des institutions financières états-uniennes ne lisent pas toutes les pistes sur les bandes magnétiques des guichets, ce qui augmente sensiblement le risque de fraude¹⁶⁵. Trop souvent, les mesures de sécurité mises en place sont en effet inégales: on met un quadruple verrou sur la porte en acier trempé de l'entrée principale, mais on laisse la fenêtre de la cave ouverte.

Les fraudeurs se spécialisent dans la recherche du point faible, et ils le trouvent parfois là où aucun des concepteurs de systèmes n'aurait songé à vérifier. Au cours des derniers mois, par exemple, on a constaté aux États-Unis que les systèmes informatiques de certains détaillants conservaient en mémoire le numéro d'identification personnel de clients ayant effectué un paiement au point de vente, même si les règles des réseaux de paiement leur interdisent de saisir ce numéro, et plus encore de le conserver. Il a suffi à des criminels de pénétrer dans les systèmes de ces détaillants pour glaner tous les renseignements requis pour commettre des fraudes qui auraient touché jusqu'à six cent mille (600 000) personnes¹⁶⁶.

¹⁶³ Schneier, Bruce. *Schneier on Security*, blogue, page du 26 septembre 2005, au www.schneier.com/blog/archives/2005/09/fingerprint-loc.html.

¹⁶⁴ *UK detects chip-and-pin security flaw*. Card Forum, 6 mai 2006, au www.cardforum.com/printarticle.html?id=20060605TS17BFMS&from=home.

¹⁶⁵ Wolfe, Daniel. *Magnetic-Stripe Data Underused, ATM Report finds*. American Banker on line, 2 août 2005. Bergstein, Brian. *Analysts say ATM systems highly vulnerable to fraud*. Bank Systems & Technology online, 2 août 2005. Disponible au www.banktech.com/showArticle.jhtml?articleID=167100238.

¹⁶⁶ Sullivan, Bob. *Debit card thieves get around PIN obstacle*. MSNBC.com, 9 mars 2006; Wolfe, Daniel; Lindenmayer, Isabelle. *PIN Debit Breach Update: What You Need to Know*. American Banker online, 13 mars 2006.

Et si la mesure de la fréquence des frappes sur un clavier peut constituer un authentifiant biométrique, l'enregistrement du son que font les touches du clavier peut permettre à lui seul de reconstituer avec un haut degré de précision ce qui est dactylographié – et qui peut inclure des informations comme des mots de passe¹⁶⁷. On sait d'autre part depuis plus de vingt ans qu'il est également possible de saisir l'information traitée sur un poste informatique en captant les ondes électro-magnétiques qu'il émet¹⁶⁸.

La volonté de passer à l'authentification à deux facteurs ne suffit pas quant à elle à décourager les escrocs, qui cherchent activement à adapter leurs tactiques d'hameçonnage¹⁶⁹.

B- Trouver l'équilibre

Les systèmes d'authentification devraient être conçus pour mitiger les risques à l'égard des banquiers comme de leurs clients et des commerçants bénéficiaires d'un paiement. Or il y a lieu de craindre que ce n'est pas ce qui se produit. Il y a non seulement souvent déséquilibre en faveur du banquier, mais même parfois mauvaise gestion du risque par ce dernier.

D'abord et par exemple en matière de commerce électronique, le commerçant requiert dans bien des cas plus de renseignements qu'il ne le faudrait: on peut songer aux cas où on requiert l'identité précise d'un client potentiel avant qu'il puisse être informé, par exemple, des modes de paiement disponibles¹⁷⁰. Dans un tel contexte, le commerçant court des risques d'exploitation variés: d'abord, il peut perdre un client potentiel agacé par ce processus. Ensuite, il recueille des renseignements qui s'avéreront parfois inexacts: le quart des internautes états-uniens (24%) admettent avoir déjà fourni un pseudonyme ou d'autres données falsifiées afin d'éviter de divulguer certains renseignements personnels à

¹⁶⁷ *Researchers snoop on keyboard sounds – computer eavesdropping yields 96 percent accuracy rate.* CNN.com, 21 septembre 2005, au us.cnn.com/2005/TECH/internet/09/21/keyboard.sniffing.ap/index.html.

¹⁶⁸ van Eck, Wim. *Electromagnetic Radiation from Video Display: An Eavesdropping Risk?* Computers & Security 4 (1985) 269-286. Disponible au www.shmoo.com/tempest/emr.pdf.

¹⁶⁹ *Phishers Beat Citi's Two-Factor Authentication.* Bank Systems & Technology, 18 juillet 2006. Disponible au www.banktech.com/showArticle.jhtml?articleID=190500614.

¹⁷⁰ Beaucoup de sites web marchands sont en effet conçus de telle manière qu'on ne peut inventorier les méthodes de paiement disponibles sans fournir une identité et désigner un bien qu'on voudrait acquérir. On consultera par exemple, et à titre strictement illustratif, des sites comme ceux des sociétés amazon.com, Indigo.ca ou fnac.com.

l'exploitant d'un site web¹⁷¹. En troisième lieu, le commerçant augmente la quantité de renseignements qu'il doit traiter, conserver et protéger.

Bref, les pratiques du commerçant qui devraient viser en principe à réduire son risque juridique par la collecte des renseignements véritablement pertinents ont pour effet d'ajouter au risque juridique (en cas de vol des renseignements, notamment) et aux risques opérationnels qu'il encourt. En somme, il accroît ses coûts et ses risques, sans qu'il soit manifeste qu'il en retire un avantage significatif.

Cela dit, ces risques demeurent relativement spéculatifs: la probabilité qu'ils surviennent ne paraît pas extrêmement élevée. Par contre, ils peuvent s'avérer dans certains cas extrêmement coûteux: on peut par exemple penser à une situation où, en raison d'un vice de conception, un site web laisserait assez facilement «fuir» au bénéfice d'un pirate des dizaines de milliers de numéros de cartes de crédit. La faute du commerçant pourrait potentiellement l'exposer à des réclamations ruineuses, surtout s'il s'agit d'une entreprise de taille modeste.

Le consommateur, lui, tire le plus souvent assez peu d'avantages des pratiques reliées à l'authentification, à moins qu'elles soient extrêmement limitées dans leur portée. D'abord, il ne dispose habituellement pas de modes d'identification du commerçant qui soient absolument fiables, d'où notamment le problème de l'hameçonnage. Les informations qui lui permettraient d'évaluer le risque qu'il encourt en visitant un site donné ne sont généralement pas disponibles: pensons par exemple à la description des mesures de sécurité mises en oeuvre par l'exploitant. Bien entendu, il ne participe en aucune manière à la conception, à la construction et à l'exploitation des processus d'authentification mis en oeuvre par les commerçants¹⁷².

L'évaluation de la qualité des mesures de sécurité mises en place par les commerçants est par ailleurs compliquée, sinon compromise, par leur propension à arguer que le secret est le garant de la sécurité: s'ils ne révèlent rien de leurs mesures, les escrocs ne pourraient les percer, tandis que la transparence n'aurait d'autre résultat que d'exposer leurs vulnérabilités à quiconque voudrait les exploiter. Cela ne laisse guère d'espace pour des débats éclairés. Cette analyse chérie par les entreprises est pourtant depuis longtemps

¹⁷¹ Fox, Susannah *et al.* *Trust and privacy online: Why Americans want to rewrite the rules*. Washington, Pew Internet & American Life Project, 20 août 2000. 29 p. On trouvera le document (PDF) en passant par l'adresse www.pewinternet.org/reports/toc.asp?Report=19. L'échantillon était de 2 117 répondants, dont 1 017 internautes. La marge d'erreur des résultats est donc en général inférieure à 3%.

¹⁷² sinon, évidemment, dans la mesure où il obéit aux instructions reliées à ces processus et fournit des renseignements.

discréditée¹⁷³. Si elles entendent néanmoins se complaire dans une conception que certains anglophones décrivent par l'expression *security through obscurity*, il paraît légitime qu'elles assument la responsabilité qui doit accompagner des choix technologiques dont elles revendiquent la seule maîtrise.

Le consommateur ne peut non plus contrôler l'usage qui sera fait des renseignements qu'il fournit postérieurement à leur communication. Dans de nombreux cas, on lui refusera en pratique l'accès à un bien, un service ou une information s'il ne fournit pas certains renseignements.

En somme, le consommateur dépourvu de contrôle court presque assurément un risque, encore que l'ampleur des conséquences qu'il peut entraîner sera le plus souvent modérée. Ces conséquences peuvent néanmoins s'avérer, à l'occasion, catastrophiques¹⁷⁴.

On se trouve donc dans une situation où la partie qui participe le moins aux processus de décision à l'égard des risques liés au fonctionnement d'une fonction, et qui peut le moins les évaluer ou s'en prémunir, court le plus souvent des risques.

C- Biométrie et autres solutions

Deux constats s'imposent: les technologies biométriques ne seront pas plus infaillibles que les autres, et on pourrait améliorer la sécurité de nombreux systèmes autrement – et peut-être plus simplement – qu'en recourant à la biométrie. Quant au premier énoncé, citons Schneier, qui l'illustre de manière claire et concise:

«A keyboard fingerprint reader can be similar. If the verification takes place across a network, the system may be insecure. An attacker won't try to forge Alice's real thumb, but will instead try to inject her digital thumbprint into the communications.

¹⁷³ en vertu notamment du principe de Kerckhoff, formulé en 1883 et bien connu en cryptographie: la sécurité d'un système ne doit pas dépendre du secret entourant la structure du système. Ce secret ne peut en effet être maintenu. Au contraire, la transparence à cet égard permet aux tiers d'éprouver le système et d'en publier les failles, ce qui contribue à le renforcer. À cet égard, par exemple, Anderson, Ross. *Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore*, Cambridge, 2002, 13 p. On trouvera cette étude au www.net-security.org/article.php?id=145.

¹⁷⁴ Comme dans le cas d'un vol d'identité assorti de dettes considérables et d'actes criminels apparemment commis par l'individu dont l'identité a été volée.

The moral is that biometrics work well only if the verifier can verify two things: one, that the biometric came from the person at the time of verification, and two, that the biometric matches the master biometric on file. If the system can't do that, it can't work. Biometrics are unique identifiers, but they are not secrets. You leave your fingerprints on everything you touch, and your iris patterns can be observed anywhere you look.

Biometrics also don't handle failure well. Imagine that Alice is using her thumbprint as a biometric, and someone steals the digital file. Now what? This isn't a digital certificate, where some trusted third party can issue her another one. This is her thumb. She has only two. Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation.

And biometrics are necessarily common across different functions. Just as you should never use the same password on two different systems, the same encryption key should not be used for two different applications. If my fingerprint is used to start my car, unlock my medical records, and read my electronic mail, then it's not hard to imagine some very unesecure situations arising.

Biometrics are powerful and useful, but they are not keys. They are not useful when you need the characteristics of a key: secrecy, randomness, the ability to update or destroy. [...]»¹⁷⁵

Les milieux bancaires déploient par ailleurs déjà d'autres méthodes que les techniques biométriques pour faciliter l'authentification. Au Canada, les réseaux Interac,

¹⁷⁵ Schneier, Bruce. *Biometrics: Uses and Abuses*. Inside Risks 100, Communications of the ACM, vol. 42, n 8, août 1999. Disponible au www.schneier.com/essay-019.html.

Visa et MasterCard ont déjà annoncé qu'on remplacerait d'ici 2015 toutes les cartes à bande magnétique par des cartes à puce. Si les milieux financiers britanniques ont annoncé que le passage à la carte à puce y a permis de réduire la fraude dans une proportion de treize pour cent (13%)¹⁷⁶, Les détaillants canadiens s'inquiètent pour leur part vivement de l'investissement de dizaines de milliards de dollars qu'ils devront consentir pour remplacer tous leurs lecteurs de cartes¹⁷⁷.

On utilise également de plus en plus des méthodes d'analyse de la cohérence des données pour détecter les opérations frauduleuses. Exemple simple, le système informatique d'un émetteur de carte de crédit devrait constater qu'il est improbable que le même numéro de carte serve à cinq minutes d'intervalle à effectuer des opérations de plus de mille dollars à Tokyo et à Paris, et faire obstacle au moins à la seconde.

D- Que faire?

Parce que les gens oublient leurs mots de passe¹⁷⁸ ou prêtent au voisin leur carte d'accès, on pencherait vers des processus d'authentification qu'on ne peut ni perdre, ni oublier, parce qu'ils sont en somme nous-mêmes. La tentation est grande de faire des technologies biométriques la panacée que vantent leurs fabricants.

Elles comportent pourtant des problèmes fondamentaux et sérieux. Les renseignements biométriques sont rarement secrets: ils peuvent être obtenus et imités. Le consommateur ne peut cependant pas remplacer son empreinte digitale après qu'un fraudeur s'en soit emparé, et il ne lui reste qu'au plus neuf (9) substituts utilisables avant d'être exclu... L'identifiant biométrique est difficilement révoquant, même quand il serait nécessaire de le révoquer.

Le consommateur opéré en raison d'une cataracte ne pourra peut-être pas participer à un réseau protégé par un mécanisme de reconnaissance de l'iris: il y aura des exclus. Et il y aura aussi des individus assez astucieux pour altérer leurs caractéristiques biométriques lorsque cela les arrangera.

¹⁷⁶ *Chip-and-pin 'cuts fraud by 13%'*. BBC News, 6 mars 2006, disponible au <http://news.bbc.co.uk/go/pr/fr/2/2/hi/business/4779314.stm>.

¹⁷⁷ Trichur, Rita. *Chip cards to cost billions; retailers worry costs could outweigh benefits*. Canoe Network, 16 avril 2006, disponible au <http://money.canoe.ca>.

¹⁷⁸ et qu'ils deviennent de toute manière de plus en plus faciles à percer informatiquement: *Biometrics becomes a commodity*. Bank Systems & Technology online, 1er février 2006, disponible au www.banktech.com/showArticle.jhtml?articleID=177105253.

Malgré les promesses des fabricants, les technologies biométriques comportent ou bien des taux élevés d'authentification erronée, ou bien des exigences d'utilisation qui les rendent très peu commodes. Il n'existe de toute manière que très peu d'évaluations d'expériences pratiques sur des populations de plusieurs millions de personnes, qui permettraient de valider vraiment l'efficacité de ces méthodes.

D'autre part, les processus d'obtention et de vérification des données sont, et demeureront, relativement coûteux, même si d'éventuels déploiements à grande échelle abaissent le coût des matériels. Ils constituent aussi l'une des plus grandes vulnérabilités de cette approche: il suffit en effet qu'une personne s'identifie faussement dès l'étape initiale d'enregistrement dans un système, pour pouvoir ensuite procéder impunément à des opérations.

Les techniques offertes par divers fabricants sont par ailleurs de qualités et de coûts très différenciés, mais rien n'assure que des entreprises déploieront des matériels de très haute qualité. On n'en est pas non plus au stade où l'interopérabilité des différents produits proposés soient tels qu'ils puissent être reliés les uns aux autres. Par conséquent et même si toutes les banques décidaient par exemple de passer à l'identification dactyloscopique au guichet automatique, rien ne garantirait *a priori* que l'empreinte captée dans un guichet de la Banque Nationale pourrait être traitée par la Banque Royale, par exemple¹⁷⁹.

Bref, la biométrie n'est surtout pas infaillible. Elle peut donc servir d'appoint, mais beaucoup s'entendent pour dire qu'elle ne peut remplacer à elle seule les autres méthodes d'authentification. Opter pour la biométrie seule serait donc téméraire, tandis qu'ajouter la biométrie à des processus déjà en place prend des allures d'investissement hasardeux dans des solutions qui pourraient s'avérer impopulaires.

On en revient à la gestion des risques. Pour contrôler le risque juridique ou le risque de crédit, jusqu'où sera-t-on prêt à accroître le risque réputationnel et, peut-être, le risque d'exploitation? Minimiser les pertes, mais au prix de la colère de la clientèle, de coûts administratifs et de risques de pannes? Posé dans ces termes, le choix de la biométrie paraît moins tentant.

¹⁷⁹ Si d'aventure l'industrie bancaire devait décider de recourir à la biométrie en réseau, on peut croire qu'elle résoudrait ces problèmes, mais on ne peut exclure que des institutions se lancent avant les autres et adoptent à grands frais des systèmes qui ne seraient pas facilement compatibles.

Certains envisagent malgré tout de déployer à grande échelle des techniques biométriques¹⁸⁰, même dans le secteur financier; quelques-uns l'ont même déjà fait. Dans pratiquement tous les cas, on bâtit ainsi des systèmes centralisés et fragiles. Peut-être faut-il par conséquent repenser les architectures elles-mêmes

En définitive, il s'agit de bien cerner l'ensemble des risques. On paraît à ce stade si peu maîtriser les technologies, si peu capables d'en quantifier l'efficacité, qu'on n'en est même pas à évaluer les risques juridiques qui pourraient être associés à leur déploiement, et qui sont considérables.

L'invention de nouvelles formes d'identification véritablement efficaces ne sera pas simple, parce qu'il ne s'agit pas que de régler une difficulté technique. Il faut repenser la conception qu'on se fait de l'humain dans la société, qui se trouve présentement profondément marquée par le paradigme mécaniste. On lui doit des idées d'une extraordinaire importance, comme celle de l'autonomie des individus, ayant des droits propres; mais on lui doit aussi une vision atomisante, qui réduit la personne à être une pièce de la machine sociale, dont le comportement «normal» se trouve nécessairement prévisible et explicable, réglable.

L'envoûtement que semblent exercer la biométrie et quelques autres technologies tient sans doute en bonne part à l'impression qu'il s'agirait d'un ensemble de méthodes pratiquement infaillibles. La révélation qu'elles comportent leur part d'erreurs, ou qu'on ne sait pas vraiment dans quelle mesure elles sont fiables, rompt le charme.

¹⁸⁰ et peut-être même massivement: la politique officielle du gouvernement des États-Unis veut par exemple toujours, au moment d'écrire ces lignes, que toute personne entrant sur le territoire de ce pays (à compter d'une date toutefois sans cesse reportée) soit contrainte de fournir un identifiant biométrique. Certains États étrangers ont déjà exprimé leur vive opposition à cette politique. Si elle devait être maintenue, elle imposerait des contraintes importantes aux postes frontaliers et aux gestionnaires d'aéroports, mais aussi aux transporteurs, qui voudront contrôler eux-mêmes la validité de l'identifiant biométrique avant le départ parce que le coût de transport de l'individu refoulé à la frontière des États-Unis leur sera imputé, compte tenu de l'article 148 de la *Loi sur l'Immigration et la Protection des réfugiés*, L.R.C., c. I-2.5 et de l'article 273 du *Règlement sur l'Immigration et la Protection des réfugiés*, DORS 2002-227. Cette dernière politique, appliquée depuis la fin des années 1980 par de nombreux États, dont le Canada, constitue à la fois un remarquable exemple de privatisation effective par sous-traitance non rémunérée d'une fonction essentiellement étatique, i.e. le contrôle des frontières, et d'impartition d'une fonction d'authentification à des milliers de préposés de transporteurs qui ne sont pour la plupart pas adéquatement formés pour effectuer une tâche qui, dans certains cas, peut s'avérer fort délicate et complexe.