*Noëlle Lenoir**

PROTECTION DES DONNÉES : LE MATCH EUROPE / ÉTATS-UNIS

Bien avant que le mot « Ubérisation » ne fasse son entrée dans le vocabulaire courant, la dématérialisation des moyens de paiement avait déjà passablement bouleversé les pratiques du monde de la finance, de l'industrie et du commerce. Paiements à distance par Internet ou sur mobile reliés à une carte bancaire, paiement par Paypal liant portefeuille électronique et compte bancaire, et maintenant paiement sans contact par carte ou sur mobile : la croissance du e-commerce comme du commerce de proximité s'appuie de plus en plus sur l'électronique, devenue le sésame de la consommation de masse.

La création du GIE des cartes bancaires dans les années 1980 y a sans doute contribué. Il n'en reste pas moins que la France est relativement bien placée au sein de la sphère de la finance numérique. Elle occupe la 6e place dans le monde derrière le Royaume-Uni à la 3e place et l'Allemagne à la 5e. Le gouvernement a lancé en octobre 2015 une « stratégie nationale des moyens de paiement » afin de renforcer encore la compétitivité de la filière des paiements par l'innovation. Car là est l'enjeu : les moyens de paiement électronique ne sont pas seulement une facilité pour le consommateur et, donc, un élément incontournable pour les secteurs de la finance et du commerce. Ils sont surtout porteurs d'innovations qui représentent un capital potentiel d'influence considérable. Point n'est besoin d'être grand clerc pour comprendre que celui qui est en mesure de définir les standards des moyens de paiement et le *business model* auxquels ils renvoient a le pouvoir de peser sur toutes les transactions financières et, partant, sur l'ensemble de l'économie des échanges.

* Membre du Conseil constitutionnel entre 1992 et 2001, puis ministre chargée des Affaires européennes de 2002 à 2004 dans le gouvernement de Jean-Pierre Raffarin. Noëlle Lenoir s'est aussi intéressée de près aux questions relatives à la protection des données personnelles lors de son passage à la Commission nationale de l'informatique et des libertés (CNIL). Juriste de formation, elle est associée au cabinet d'avocats Kramer Levin Naftalis & Frankel.

L'intérêt des GAFA

Ce n'est pas un hasard si les géants de l'Internet — les fameux GAFA, Google, Apple, Facebook et Amazon —, toujours prompts à proposer des innovations pour asseoir leur position sur le marché, s'y intéressent de près : Google avec son Google Wallet, Apple avec ApplePay et Amazon avec son projet de paiement par reconnaissance faciale *via* un selfie, déjà lancé par d'autres opérateurs comme la Banque postale en France et MasterCard aux États-Unis. Si l'Union européenne s'attache, depuis quelques années, à mettre en place un véritable marché intégré des services de paiement, c'est, dans le cadre de l'achèvement du marché intérieur, pour en développer les performances technologiques de manière à rivaliser avec les concurrents américains.

Alors que la sécurisation des paiements ne semblait pas jusqu'ici la préoccupation première de nos voisins d'outre-Atlantique, les Européens, eux, entendent s'adresser aux consommateurs qui montrent encore une certaine méfiance vis-à-vis du paiement en ligne et consolider ainsi leur avance en matière de sécurité des transactions sur le web. Celle-ci est loin d'être parfaite. Chacun sait que le hacking est l'un des sports les plus répandus de nos jours. Il permet d'organiser des escroqueries de grande ampleur ou de servir un but plus politique : sensibiliser le public à la vulnérabilité de certains systèmes, par exemple. Nouveau paradigme, le hacking constitue un danger majeur en même temps qu'une formidable incitation à prendre de court les pirates en inventant de nouveaux dispositifs de sécurité inexpugnables.

À cet égard, l'Europe s'impose. Et elle le fait autant à travers sa technologie que par sa culture de la « *privacy* » que traduit une législation sur la « protection des données » particulièrement contraignante pour les entreprises. Or l'application extraterritoriale de cette législation influe sur les rapports commerciaux, voire politiques, entre l'Union européenne et les États-Unis. Au point de conduire ces derniers à modifier leur propre cadre juridique. Habituellement, ce sont les législations américaines qui, de par leur portée extraterritoriale, conduisent les Européens à adapter leur corpus législatif. Ce fut le cas de la loi Sarbanes-Oxley de 2002, qui a obligé les banques européennes à se doter d'un arsenal de *compliance*. Son efficacité n'a pas été avérée au moment de la crise systémique bancaire de 2008 mais, pour autant, il a profondément changé le fonctionnement interne des établissements de crédit. Cette fois-ci, ce sont les États-Unis qui sont appelés à réagir et à se plier aux exigences de protection des données résultant

de plusieurs arrêts de la Cour de justice de l'Union européenne (CJUE) rendus en 2014 et 2015.

Le marché intérieur des services de paiement : un enjeu stratégique pour l'Europe

Le marché intérieur européen des paiements à distance a pu être mis en place par une réglementation laissant très peu de marge de manœuvre aux États. La directive de 2007, révisée en 2015, sur les services de paiement est en effet un texte d'harmonisation totale. Ce qui signifie que les États, en dehors de quelques exceptions limitées, ne peuvent ni y déroger ni en moduler les prescriptions. La directive a décloisonné les marchés nationaux tout en ouvrant une brèche dans le monopole des banques, en permettant à d'autres acteurs agréés — les établissements de paiement et les établissements de monnaie électronique — de les concurrencer.

Il est intéressant de noter que la directive du 8 octobre 2015 modifiant la directive de 2007 insiste surtout sur la sécurité des paiements, « fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique ». L'expérience a montré, en effet, que si le e-commerce croît de façon appréciable, il lui reste à conquérir la confiance pleine et entière des consommateurs en trouvant les moyens de lutter contre les intrusions frauduleuses.

La solution préconisée par le texte est le cryptage incorporé aux dispositifs personnels du payeur (lecteurs de cartes, mobiles) ou fourni par le prestataire de services de paiement, par SMS ou courriel. Le législateur européen prescrit une « authentification forte du client » qui repose, d'une part, sur un élément que l'utilisateur seul connaît (la réponse à une question personnelle) et, d'autre part, sur un élément qui lui est inhérent. La Commission nationale de l'informatique et des libertés (CNIL) est de plus en plus vigilante à cet égard. Dans des délibérations récentes, elle a chapitré des entreprises qui donnaient accès à leurs systèmes *via* de mots de passe trop facilement détectables, en dehors même de toute réglementation spécifique comme en matière de paiements électroniques. Facebook l'a expérimenté à ses dépens, en février 2016, à l'occasion d'une mise en demeure de la CNIL qui lui reprochait l'utilisation de mots de passe non conformes.

Parallèlement, les prestataires des services de paiement se doivent de collecter des informations de plus en plus détaillées aux deux bouts de la chaîne, tant sur le donneur d'ordre que sur le

destinataire du transfert de fonds, dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme. Un nouveau règlement de 2015, qui forme un quatrième « paquet anti-blanchiment », impose en effet d'assurer la traçabilité des paiements. Ces prestataires sont désormais responsables du traitement de données sensibles justifiant des mesures de sécurité renforcées.

Les paiements au défi du hacking

Sorte d'Arsène Lupin des temps modernes, le hacker est à la fois escroc et héros. Il est héros car il utilise la ruse et non la force pour s'introduire dans des systèmes pour en capter les données qui vont éventuellement faire sa fortune. Il est escroc, tant il est vrai que les sommes détournées peuvent être gigantesques. En dehors du cas particulier des prestataires de services de paiement, nulle entreprise, nulle administration n'est épargnée par cette pratique. On peut dire qu'en réalité il y a aujourd'hui deux catégories d'entreprises : celles qui s'aperçoivent que leurs systèmes ont été piratés et celles qui ne s'en aperçoivent pas.

L'une des affaires de piratage les plus spectaculaires, révélée en 2014, est le vol des données de plus de 110 millions de cartes bancaires de clients de la chaîne Target, deuxième groupe de la grande distribution aux États-Unis. Les hackers avaient utilisé des logiciels malveillants (*malwares*) capables d'intercepter les données des clients du magasin au moment où elles transitent par la mémoire vive d'un ordinateur. Comme elles n'étaient pas cryptées, la manœuvre était facile.

Une autre affaire retentissante concerne un pirate turc, arrêté en Allemagne en 2013, puis extradé aux États-Unis pour y être jugé. En clonant des cartes bancaires, il était parvenu à dérober des dizaines de millions de dollars dans des distributeurs automatiques de billets. L'argent volé était placé dans des comptes *offshore* et transformé en monnaie électronique.

L'Europe a un temps d'avance en matière de sécurité

Ces deux exemples parmi d'autres ont mis en évidence le caractère quelque peu archaïque du système des cartes bancaires aux États-Unis, dont les informations sont stockées sur une simple piste magnétique au lieu d'être contenues dans des puces informatiques beaucoup plus difficilement duplicables. Le piratage mafieux, pratiqué souvent à partir des pays d'Europe centrale

et orientale, représenterait ainsi environ 11 milliards de dollars chaque année.

L'ampleur de la fraude est, semble-t-il, bien moins importante en Europe qu'aux États-Unis. De plus, jusqu'à une période récente, il n'existait pas aux États-Unis d'autorité de protection des données comparable à la CNIL qui fût en mesure de demander des comptes, par exemple lors d'audits inopinés, aux opérateurs négligents (et donc indirectement responsables du vol des données), et de leur infliger le cas échéant des sanctions administratives. Ce vide juridique vient d'être partiellement comblé. En 2015, une cour d'appel américaine a décidé que la Federal Trade Commission (FTC), chargée de la protection du consommateur, avait compétence pour poursuivre et sanctionner les entreprises manquant à leur obligation d'assurer la confidentialité des données personnelles qui leur sont confiées. La FTC avait poursuivi pour négligence la chaîne des hôtels Wyndham qui se bornait à stocker les données des cartes bancaires des clients sans aucune protection, de sorte que des hackers avaient pu aisément s'emparer en 2008 et 2009 des données de plus de 600 000 personnes.

En Europe, les banques expérimentent une nouvelle génération de cartes bancaires dotées d'un cryptogramme « dynamique », c'est-à-dire éphémère et se renouvelant à intervalles réguliers (par exemple, toutes les 20 minutes) pour prévenir les utilisations frauduleuses.

Le droit des données, source d'avantage compétitif ?

L'histoire explique pour partie les différences d'approche en matière de sécurité informatique de part et d'autre de l'Atlantique et, d'une manière plus générale, de protection des données. Les États-Unis n'ont pas connu la dictature sur leur sol, contrairement aux États de l'Europe continentale. D'où la sensibilité des citoyens européens à la protection de leur vie privée et de leurs données personnelles. Deux événements récents ont, en outre, renforcé la volonté de l'Europe d'assurer cette protection où que ce soit dans le monde. Le premier est le traité de Lisbonne et la charte des droits fondamentaux de l'Union européenne qui en fait partie intégrante. Désormais, la protection des données personnelles, droit fondamental de l'Union, est la base juridique de toute législation en la matière, alors que la directive du 24 octobre 1995 sur la protection des données, applicable jusqu'en 2018, se fondait sur le marché intérieur et la nécessité d'y favoriser la libre circulation des données.

Le second événement est l'affaire Snowden, du nom de cet agent contractuel de la National Security Agency (NSA) qui a fait fuiter des millions de données top secret pour dénoncer à la face du monde les pratiques de surveillance de masse de l'agence. Il y a quelques années, Edward Snowden aurait été considéré simplement comme traître à sa patrie. Aujourd'hui, pour certains, il est presque un démiurge, légitimement habilité à donner des leçons de démocratie au gouvernement américain depuis la Russie où il s'est enfui. L'écho recueilli par Snowden dans l'opinion publique et au Parlement européen s'est directement traduit dans la jurisprudence de la CJUE dont on sait l'influence décisive en Europe, liée au fait qu'elle a le dernier mot.

En vertu de cette jurisprudence — en particulier les arrêts Google Spain du 14 mai 2014 et Weltimmo du 1er octobre 2015 —, il est clair que toutes les données concernant des Européens (y compris des données bancaires) traitées ou stockées aux États-Unis sont sous la protection du droit de l'Union, pour peu que l'opérateur ait un « établissement » en Europe. Ce que confirme le futur Règlement général sur la protection des données, appelé à remplacer en 2018 la directive de 1995. Selon ce texte, en matière commerciale, le critère d'applicabilité de la loi européenne n'est pas le lieu de traitement des données, mais la qualité de résidents dans l'Union des personnes dont les données sont traitées.

De manière plus illustrative encore, dans son arrêt Schrems du 6 octobre 2015 — du nom de l'étudiant en droit autrichien disciple de Snowden —, la Cour a invalidé la décision de la Commission européenne sur le *Safe Harbor*, l'accord conclu entre l'Union européenne et les États-Unis, rendant dès lors immédiatement illégaux les transferts de données effectués dans ce cadre. Le motif : les services américains peuvent puiser dans les données stockées aux États-Unis par les acteurs de l'Internet tels que Facebook en infraction au droit européen de la protection des données. Le fait que certains opérateurs américains (Google, Facebook, Microsoft…) aient installé des *clouds* en Europe n'est pas étranger au souci de rassurer le consommateur européen, tout en ne se faisant pas distancer par des opérateurs européens prompts à occuper le créneau de la sécurité des données, censée selon eux être moins bien assurée aux États-Unis.

Tensions Europe / États-Unis

Il y a, dans la tension née de cette jurisprudence entre les États-Unis et l'Europe, beaucoup de non-dits. Il est évident que

les Européens, qui ne prétendent pas appliquer les critères de la jurisprudence Schrems pour arrêter les transferts de données entre l'Union européenne et la Chine, par exemple, y voient aussi un levier pour rapatrier en Europe des *data centers* dotés de toutes les technologies de sécurité les plus avancées. Le but est de positionner ainsi leurs opérateurs du numérique en tête du marché de la sécurité des systèmes et des données.

Le nouvel accord *Privacy Shield*, conclu en février 2016 entre le gouvernement américain et la Commission européenne pour résoudre ce conflit renforce notablement les garanties des citoyens européens en leur ouvrant plusieurs possibilités de recours pour contrer d'éventuels abus des services américains. Pourtant, il est déjà vilipendé par des parlementaires européens et regardé avec suspicion par le G 29, le groupe qui réunit les 28 autorités de protection des données en Europe.

De même, la bataille que se livrent actuellement Apple, d'une part, et le département de la Justice américain et le FBI, d'autre part, est pleine d'enseignements. Le refus opposé par Apple de fournir l'accès aux données de l'iPhone du terroriste islamiste qui a tué, en décembre 2015, 14 personnes à San Bernardino en Californie pourrait ne pas être seulement lié au souci du dirigeant de la compagnie, Tim Cook (1), de « ne pas mettre en danger » les innombrables utilisateurs de ses mobiles dans le monde. Apple, par là même, devient le centre des débats sur les enjeux de la sécurité des données et la protection de la vie privée des citoyens...

Comment concilier sécurité des données et sécurité tout court, alors que le terrorisme frappe au cœur des démocraties ? Et comment va se terminer cette course-poursuite entre les Européens et les Américains sur le marché du numérique et spécialement de la sécurité des données ? Comment les uns et les autres peuvent-ils en finir avec le hacking, nouveau vecteur d'une corruption transfrontalière en pleine expansion ? L'avenir est encore incertain. Ce qui est sûr, en revanche, c'est que, une fois encore, contrairement à une idée reçue, c'est le droit — ici celui de la protection des données opposé à celui de la protection de la sécurité publique — qui façonne les technologies, et non l'inverse. Encore faut-il éviter que les contraintes trop souvent tatillonnes qui pèsent sur les opérateurs en matière de protection des données n'entravent la compétitivité de l'industrie au lieu de la renforcer.

---

(1) Voir l'interview de Tim Cook dans *Time Magazine* du 17 mars 2016.