N°16 / FÉVRIER 2016

LES CARNETS DE L'ÉCONOMIE ET DE L'ENTREPRISE

Notre lettre aux parlementaires

ÉDITO

L'IDENTITE NUMERIQUE, PIERRE ANGULAIRE DE LA MODERNISATION DE L'ETAT ET DE L'ECONOMIE

Ce numéro des Carnets est exclusivement consacré au numérique. Nous le traitons sous deux angles complémentaires.

Tout d'abord, nous décrivons et analysons les raisons du succès de la politique de déploiement de l'identité numérique menée en Suède et en Estonie. L'identité numérique est généralisée dans ces deux pays ; elle sert tout à la fois à gérer les informations publiques (carte d'identité, permis de conduire, santé, écoles, ...) et à permettre des transactions commerciales privées.

Dans les deux cas, le succès considérable de cette numérisation de la société résulte de la combinaison de trois facteurs :

- En premier lieu, **une volonté politique forte**, passant en particulier par la numérisation des services publics et de nombre d'actes administratifs.

- Deuxièmement, **le choix de confier la totalité de l'investissement, la mise en œuvre opérationnelle et l'exploitation à un consortium formé d'opérateurs privés, sous contrôle de la puissance publique**. Il est, à ce propos, à noter que les banques de réseau sont un élément indispensable de ces consortia parce qu'elles disposent d'un maillage fin du territoire, qu'elles savent gérer l'identité de leurs clients et enfin parce qu'elles disposent de systèmes d'information très puissants. L'équilibre économique d'exploitation est atteint en combinant les ressources liées à la consultation des bases de données et à l'exploitation commerciale du réseau.

- Enfin, **les gouvernements ont défini et effectivement mis en œuvre une politique claire et stricte de respect de la confidentialité des données personnelles** (en particulier concernant la santé) et de contrôle de l'utilisation des données privées à des fins commerciales. L'instauration d'un régime de confiance fondé sur un encadrement juridique strict est une composante essentielle du succès des opérations en Suède et en Estonie.

Dans une seconde partie, nous dressons un rapide panorama du cadre juridique - lois, mesures réglementaires, jurisprudence... - en train de se mettre en place aux Etats-Unis en matière de cybersécurité, un sujet désormais considéré comme majeur par les autorités américaines compte tenu des enjeux économiques, stratégiques et politiques cruciaux soulevés par la protection des systèmes d'information.

Nous reviendrons bien sûr, dans de futurs numéros des Carnets, sur d'autres aspects des enjeux liés au numérique.

Philippe-Olivier ROUSSEAU
philippe-olivier.rousseau@bnpparibas.com
Affaires publiques France - BNP Paribas

UNION EUROPÉENNE

L'IDENTITE NUMERIQUE EN ESTONIE ET EN SUEDE : NOUVELLE CITOYENNETE, NOUVEAUX ENJEUX ECONOMIQUES

Le pouvoir de désigner un individu, de le distinguer de son concitoyen et d'établir avec certitude l'ensemble des attributs qui forment son identité est traditionnellement considéré comme l'une des prérogatives fondamentales de l'Etat régalien. Cependant, alors que de nombreux éléments de notre vie privée et professionnelle font désormais appel aux technologies numériques, l'idée que **l'identité puisse allier des fonctions classiques d'état civil à des opportunités économiques élargies, en étant à la fois dématérialisée et sûre, semble devoir s'imposer**.

En 2014, la Suède - dont la population était de 9,7 millions - comptait plus de 6,5 millions d'utilisateurs d'« e-identité » actifs. La même année, 1,2 millions de citoyens estoniens, soit 90% de la population du pays, étaient équipés d'une carte d'identité numérique (« e-ID card »).

Estonie et Suède, deux pionniers de l'identité numérique

C'est un constat identique, fait à la fin des années 90, qui a poussé ces deux pays, géographiquement proches mais culturellement différents, à s'engager dans la voie de l'identité numérique : un besoin urgent **de rationaliser la gestion des finances publiques tout en saisissant l'opportunité du numérique pour développer l'économie.**

En Estonie, le point de départ a lieu en 2000 avec la loi sur la signature électronique qui a instauré pour la première fois au monde une « citoyenneté électronique ». **Mais le tournant complet s'opère en janvier 2002, date à partir de laquelle les citoyens sont dotés d'une carte d'identité électronique sécurisée, l' « e-ID card »**, et ce dès l'âge de quinze ans. **Une puce est intégrée à chaque carte, comprenant deux certificats et les clefs privées de sécurité correspondantes : l'une sert à l'authentification du citoyen, la seconde à sa signature digitale, qui a en Estonie valeur juridique au même titre qu'une signature manuscrite**.

Les possibilités ouvertes par la généralisation de l'e-ID card couvrent la quasi-totalité du champ des services publics « classiques » (identification des citoyens, carte Vitale, permis de conduire, document de voyage au sein de l'UE, carte électorale, administration fiscale) mais aussi l'accès au dossier médical et aux e-ordonnances délivrées par les médecins. En parallèle, un nombre important de services privés, dont la carte bancaire, sont également accessibles aux citoyens. Quatre procédures sont exclues du dispositif : le mariage, le divorce, l'achat et la vente de biens immobiliers et l'ouverture initiale d'un compte bancaire.

La Suède suit un processus proche. La loi ne rendant aucun document d'identité obligatoire dans le pays, le vide juridique existant pour les documents d'identité physique a longtemps été pallié par la cohabitation entre différents documents reconnus (permis de conduire, passeport) par les autorités. Mais le développement de l'internet, la nécessité de fournir une identification hautement sécurisée pour les transactions financières et la volonté de simplifier l'administration du pays ont mené à **l'émergence d'une identité numérique à partir de 2003, rapidement adoptée par 80% des citoyens suédois. Elle permet tout à la fois l'identification et la signature électronique, de façon similaire à l'e-identité estonienne**.

Simplification administrative et rationalisation des finances publiques

En Estonie comme en Suède, **l'Etat a saisi l'opportunité pour mettre en place une administration numérique, clef de voûte de la numérisation du pays**. Toutes les procédures étant dématérialisées, les gains de temps et les économies d'échelles sont considérables, aussi bien pour l'administration que pour les usagers. Jaan Priisalu, ex-directeur de l'Autorité des systèmes d'information d'Estonie, estime que « chaque signature électronique équivaut à une heure libre dégagée par rapport à un processus papier (réception, compréhension, lecture, écriture, consentement, renvoi, timbrage) ».

Des partenariats public-privé indispensables au développement numérique

En Estonie, suivant sa politique de stricte rigueur budgétaire, **le gouvernement a fait le choix, au début des années 2000, d'intégrer le secteur privé à la réalisation du projet de carte d'identité électronique, dans un partenariat public-privé**. Au cœur du système, l'AS Sertifi tseerimiskeskus ou SK, le « certificate center » permet le maintien de l'infrastructure électronique nécessaire à l'utilisation des cartes. Les deux banques principales du pays, Hansabank (groupe Swedbank) et Eesti Ühisbank, en partenariat avec deux groupes des télécoms, Eesti Telefon et EMT, ont permis le développement du SK, basé sur les technologies acquises lors de la réalisation d'un centre d'authentification pour le paiement en ligne reposant sur la technologie de la « blockchain », permettant un haut niveau de sécurité. La société Trüb, rachetée début 2015 par Gemalto, a également participé à la mise en service de l'e-ID en Estonie, en assurant la sécurité numérique du projet. **Enfin, une technologie liée a été développée depuis le lancement la carte d'identité numérique, le « Mobiil-ID », qui permet aux citoyens d'accéder aux mêmes fonctionnalités par téléphone portable**.

En Suède, les banques sont un acteur historique de l'identité. Un consortium de 12 banques incluant les 4 principales banques du pays a été mandaté en 2002 par les pouvoirs publics suédois. Le Finansiell ID-Teknik BID AB a lancé dans la foulée le projet « Bank-ID », qui s'imposera rapidement comme la référence suédoise de l'identité numérique, avant de s'étendre au-delà même des frontières du pays, chez ses voisins scandinaves. Par la suite, le consortium a évolué, en intégrant des opérateurs de télécommunications et, parallèlement, en réduisant le nombre de banques. En 2014, plus de 500 millions de transactions avaient été réalisées grâce à Bank-ID, soit environ 80 utilisations annuelles par usager.

De nouvelles possibilités économiques

Outre le fait de rendre la quasi-totalité des démarches et des services publics accessibles en ligne, **l'identité numérique a permis, en Estonie comme en Suède, le développement de nouveaux secteurs économiques**. Par ailleurs, la signature électronique à valeur légale a été facteur de fluidification dans le traitement de contrats commerciaux, la création d'entreprises ou encore pour la recherche d'emploi.

L'essor numérique de l'Estonie est passé par une forte sensibilisation de la population aux enjeux liés, l'éducation au numérique dès le plus jeune âge, mais surtout le développement de l'accès à l'internet avec une ambition de « couverture totale ». **L'accès au Wifi public est d'ailleurs en passe de devenir un nouveau droit**.

La multiplication du nombre de fonds publics-privés qui accompagnent les startups depuis leur amorçage a été l'un des premiers corollaires de cette révolution de « l'e-identité », **faisant de l'Estonie le pays européen avec le plus grand nombre de startups par habitants**. La Suède n'est pas en reste, de très nombreux sites marchands, mais aussi des services publics essentiels ont saisi l'opportunité de l'identification numérique pour se développer.

Simplicité administrative, fluidification des démarches de création et de cession des entreprises et incitation à l'innovation par le numérique, ces principes, liés à la mise en place d'une identité numérique fiable, sécurisée et reconnue par l'Etat ont été le préalable à une croissance de l'économie numérique, et plus largement de tout le secteur économique pour les deux voisins de la mer Baltique. **Les deux pays ont atteint des niveaux de transactions commerciales électroniques de près de 100%, participant au développement des NFC (« Near Field Communication »). En Suède, la suppression définitive de tout type de règlement en espèces, et donc de la monnaie physique, est prévue à l'horizon 2020**.

Des enjeux fondamentaux de sécurité et de protection des données personnelles

Parallèlement aux opportunités qu'il suscite, le développement de l'identité numérique soulève des enjeux essentiels qui rendent nécessaire une régulation par les pouvoirs publics. Les gouvernements estoniens et suédois ont apporté de nombreuses garanties pour assurer un haut niveau de sécurité ainsi que la stricte protection des données personnelles.

En Estonie, celle-ci est notamment garantie par la Constitution. Par ailleurs, chaque citoyen muni de son e-ID card a accès aux informations liées à la consultation de ses données. Ainsi, le citoyen peut choisir en ligne les autorisations d'accès qu'il donne ou qu'il refuse -, par exemple aux hôpitaux pour la consultation de son dossier médical, qu'il peut choisir de mettre ou non dans la catégorie des informations accessibles sans autorisation préalable. Il est également informé des consultations de ses données par les agents de la fonction publique habilités et, en cas d'excès de leur part, il peut ouvrir un recours judiciaire. D'autre part, **le système estonien n'est pas centralisé dans une base contenant l'ensemble des données d'un individu, mais repose au contraire sur un système de demandes entre administrations (« queries »)** : le système de navigation entre les différents jeux de données X-Road accessible aux usagers.

La gouvernance numérique, permise par l'e-identification et l'e-citoyenneté, plus transparente, rend la corruption beaucoup plus difficile tout en favorisant un nombre important d'applications dédiées à la démocratie participative, en particulier par le vote électronique.

Une interopérabilité en question face aux acteurs multinationaux

L'ambition de l'Estonie et de la Suède est également de renforcer leur attractivité envers les investisseurs étrangers, notamment grâce à la simplicité administrative permise par le numérique. **La question de l'interopérabilité des identités numériques à un niveau transnational se pose donc en toile de fond du développement de la citoyenneté numérique**.

Les interactions entre les dispositifs nationaux et les autres acteurs de l'écosystème numérique, en particulier les opérateurs nord-américains souvent rassemblés sous l'acronyme GAFA - (Google Apple Facebook Amazon), doivent impérativement être précisées, Dans cette perspective, l'accord intervenu le 2 février 2016 entre les autorités européennes et nord-américaines à propos du « Safe Harbour » devra être analysé en détail . Il s'agit tout à la fois de permettre et de tenir compte des évolutions technologiques mais également de renforcer la « confiance numérique » par des standards élevés de sécurité. **Il appartient aux pouvoirs publics nationaux et européens de se saisir rapidement des enjeux de souveraineté numérique**.

Loan SANTIAGO
Affaires publiques France - BNP Paribas

ETATS-UNIS

LA CYBERSECURITE AU CŒUR DES PREOCCUPATIONS AMERICAINES

Depuis plusieurs années déjà, la cybersécurité et les conséquences que pourraient avoir des défaillances dans ce domaine sont perçues aux Etats-Unis comme étant l'une des menaces les plus sérieuses pesant sur l'économie et sur la société toute entière. De nombreuses initiatives ont en conséquence été lancées pour promouvoir la cybersécurité et répondre aussi efficacement que possible aux enjeux économiques, stratégiques et politiques soulevés par la protection des systèmes d'information. **Un cadre est ainsi progressivement en train de se mettre en place aux Etats-Unis, constitué de nouvelles réglementations, des recommandations et lignes directrices émises par les autorités publiques et de la jurisprudence issue des décisions rendues ces dernières années par les tribunaux et les superviseurs. En outre, les agences de notation, au premier rang desquelles S&P, ont indiqué que les établissements bancaires qui ne pourraient pas justifier de mesures efficaces pour lutter contre les cyberattaques pourraient voir leur note abaissée**.

« La réglementation s'étoffe lentement mais sûrement »

Dès le milieu des années 90, les Etats-Unis ont commencé à adopter des mesures législatives sectorielles en matière de cybersécurité. On peut notamment citer le « Health Insurance Portability and Accountability Act » (HIPAA) de 1996, le « Gramm-Leach-Bliley Act » de 1999 et le « Homeland Security Act » de 2002, **trois textes qui obligent respectivement les organismes de santé, les institutions financières et les agences fédérales à protéger leurs systèmes d'information**. Ces réglementations étaient cependant peu prescriptives et n'ont pu empêcher des attaques importantes contre les entreprises et les administrations américaines. L'arsenal législatif et réglementaire a donc été complété au fil des ans. Ainsi, en février 2013, estimant que la sécurité nationale et

économique des Etats-Unis dépendait du bon fonctionnement d'infrastructures dites essentielles, le Président des Etats-Unis a promulgué un « ordre exécutif »[1] relatif à la sécurité informa tique de ces infrastructures. Ce décret présidentiel prévoyait notamment que le « National Institute of Standards and Technology » (NIST), qui dépend du Département du Commerce, travaille avec les parties prenantes à l'élaboration d'un cadre volontaire de cybersécurité, connu sous le nom du NIST Framework, « destiné à permettre aux propriétaires et exploitants d'infrastructures sensibles basées aux Etats-Unis d'identifier, d'évaluer et de gérer tout risque de cyberattaque ».

Le président Obama a par ailleurs adopté début 2015 un ordre exécutif[2] visant cette fois à inciter les entreprises privées à partager davantage leurs informations sur les menaces de cyberattaques. Ce décret constituait la base d'un nouveau dispositif d' « organisations de partage et d'analyse d'informations » (ISAO), autrement dit des plateformes au sein desquelles les entreprises peuvent partager les données sur les menaces de cyberattaques entre elles et avec le Département de la sécurité intérieure (DHS - Department of Homeland Security). Dans le prolongement de ce décret, le Congrès a adopté en décembre dernier, après plusieurs années de débats, le « Cybersecurity Information Sharing Act » (CISA), un texte législatif également relatif au partage d'informations par les entreprises et qui permettra notamment d'exonérer la responsabilité de ces dernières en cas de non-respect des règles relatives à la protection des données privées. Lentement mais sûrement, la réglementation américaine s'étoffe…

« Des moyens humains et financiers de plus en plus conséquents »

Les Etats-Unis consacrent également à la prévention et à la lutte contre les cyberattaques des moyens humains et financiers de plus en plus conséquents. En 2003, dans sa « Stratégie nationale pour sécuriser le cyberespace », le président George W. Bush avait confié la responsabilité du sujet au « Department of Homeland Security », mandatant celui-ci pour élaborer des solutions nationales. En 2004, le Congrès avait décidé d'allouer presque 5 milliards de dollars à la cybersécurité, en lien avec la mise en œuvre du plan élaboré par l'administration Bush. Plus récemment, **en février 2015, le président Obama a initié la création d'une nouvelle agence fédérale dédiée à la cybersécurité, la « Cyber Threat Intelligence Integration Center » (CTIIC)**, sous la responsabilité du DNI, le directeur du renseignement américain (« Director of National Intelligence »).

« Les banques avec des contrôles de cybersécurité faibles pourraient voir leur notation abaissée »

Outre les autorités publiques, les agences de notation s'intéressent également à la cybersécurité. **Standards & Poor's (S&P) en particulier a annoncé en septembre dernier que les banques avec des contrôles de cybersécurité faibles pourraient voir leur notation abaissée, même en l'absence d'attaque**. Cette nouvelle composante de la notation S&P, qui n'a pas encore donné lieu en pratique à des baisses de notation, prendrait notamment en compte le niveau de protection des données des clients ainsi que les conséquences potentielles d'une attaque sur les résultats de l'établissement et sur sa réputation.

« La faute de l'entreprise est présumée en cas de cyberattaque réussie »

Outre les évolutions réglementaires, les décisions des tribunaux et des superviseurs fournissent également des indications quant aux règles que doivent respecter les entreprises en matière de cybersécurité, en particulier s'agissant de la protection des données personnelles de leurs clients. On peut citer à cet égard deux décisions importantes, l'une rendue par la cour d'appel de Philadelphie, l'autre par la SEC.

Par une décision rendue le 24 août 2015[3], la cour d'appel de Philadelphie, tout en consacrant la compétence de la « Federal Trade Commission » (FTC)[4] en matière de contrôle des dispositifs de cybersécurité des entreprises, a estimé que le contrôle de la FTC pouvait s'opérer a posteriori, après l'attaque, et que la FTC avait toute discrétion, lors de ce contrôle, pour décider si le dispositif de sécurité mis en place par l'entreprise pour protéger les données des clients pouvait être considéré comme « raisonnable » ou non.

Concernant la SEC, celle-ci a récemment imposé une amende de 75 000 dollars à un conseiller en investissement pour avoir manqué d'établir un dispositif « raisonnable » en matière de cybersécurité, ce manquement ayant compromis les données personnelles d'environ 100 000 personnes. Le raisonnement suivi par la SEC semble montrer que lorsqu'une attaque parvient à ses fins, il est alors présumé que les standards de sécurité de l'entreprise n'étaient pas « raisonnables » et que celle-ci doit en conséquence être sanctionnée.

Au vu de ces deux décisions récentes, il apparaît que les tribunaux et superviseurs considèrent désormais que le cadre en vigueur - lois, décrets, recommandations des superviseurs, etc. - fournit assez d'éléments d'orientation sur lesquelles les entreprises peuvent fonder leur politique de cybersécurité pour que celles-ci soient sanctionnées en cas de défaillance, au moins en ce qui concerne la protection des données des consommateurs.

Simon WINN
simon.winn@us.bnpparibas.com
BNP Paribas North America Public and Regulatory Affairs (NAPRA)

1-Executive Order « Improving Critical Infrastructure Cybersecurity », 12 février 2013

2-Executive Order « Promoting Private Sector Cybersecurity Information Sharing », 13 février 2015

3-Third Circuit rules in FTC v. Wyndham case, 24 août 2015.

4-La FTC est l'agence responsable de l'application des droits de la concurrence et de la consommation.