NUMÉRIQUE ET POLITIQUES PUBLIQUES EN FRANCE

Un virage nécessaire mais difficile

Patrick Kineider

patrick.kineider@hotmail.fr

Résumé : Depuis un quart de siècle, les progrès des NTIC (Nouvelles Technologies de l'Information et de la Communication) ont fortement impacté la vie des entreprises et les particuliers. En outre, en France, l'État lui-même a été, dans la 2e partie du XXe siècle, utilisateur de gros systèmes dans les administrations publiques, afin de mieux gérer les demandes des citoyens. Depuis le début du XXIe siècle, une nouvelle mission capitale des gouvernants est apparue : celle à la fois d'inciter aux progrès du numérique dans la vie de tous les jours et d'essayer de « réguler » l'économie, en termes de modèles d'entreprises, ainsi qu'en permettant la création d'emplois et de formations professionnelles spécialisées.

Mots-clés : Administration, économie, État, informatique, numérique, politique publique, sécurité, technologie

Le document énumère l'ensemble des domaines concernés par une politique numérique publique, en général et du strict point de vue de la sécurité des SI.
Les contenus de nombreux propos ont déjà fait l'objet, à ADELI, de billets de blogs ou d'articles de la Lettre. Il nous a cependant semblé utile de les regrouper par grands chapitres.

POLITIQUE PUBLIQUE NUMÉRIQUE : DÉCLINAISON GÉNÉRALE

On a tous fait le constat suivant. Durant les diverses phases de numérisation de la société, la recherche et le développement de solutions techniques, puis l'envahissement progressif des marchés mondiaux par des matériels manufacturés, avait pour source principale les États-Unis d'Amérique. Ce mouvement a été, en grande partie, porté par plusieurs grandes multinationales d'internet, les fameux « GAFA » (Google, Apple, Facebook, Amazon).

Malgré des formations techniques de haut niveau dans les universités, les instituts universitaires et les Écoles d'Ingénieurs, en particulier en France, l'Union européenne s'est longtemps cantonnée, dans le domaine technologique, dans un « suivisme » confortable, emboîtant le pas aux États-Unis mais en constituant un débouché de marchés. Ce n'est qu'au début du XXIe siècle que l'Asie du Sud-Est, en particulier avec la Chine et l'Inde, s'est érigée comme deuxième pôle numérique mondial.

Par ailleurs, la France est un pays du vieux continent européen. À ce titre, bien qu'ayant été par le passé, à l'origine d'inventions industrielles remarquables tels que l'électricité, le téléphone, la santé, il est coutumier d'entendre, à la fois les citoyens ou commentateurs, mais aussi les décideurs, s'exprimer ainsi en substance :

> *« nous accumulons du retard sur des pays tels que les USA »*

Citons aussi Olivier Ezratty, ancien conseil en stratégie de l'innovation :

> *« depuis 30 ans, tous les métiers ont changé avec le numérique, et cela va continuer »*

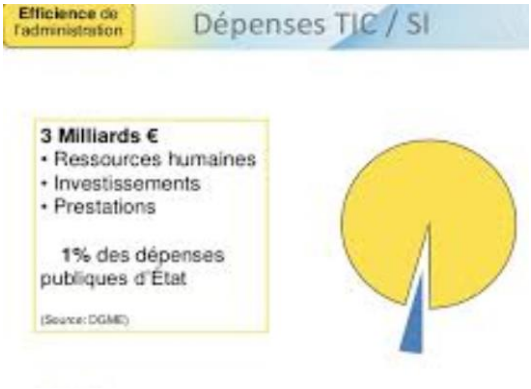
Dans notre lettre n° 106 est brièvement évoquée la « fracture numérique » qui existe dans un pays tel que la France, avec des différences d'appropriation des technologies suivant les niveaux sociaux et les équipements réseaux internet ADSL-fibre et GSM des divers territoires, bien qu'elles aient tendance peu à peu à s'estomper.

Enjeux généraux

En août 1999, à l'Université d'été de Hourtin (Gironde), le Premier ministre Lionel Jospin exposait son « programme d'action gouvernementale pour la société de l'information ». L'idée est la suivante : le numérique structure de plus en plus l'économie, l'État, les associations, et il appelle donc une gouvernance forte en termes de :

- veille technologique permanente ;
- modernisation de l'administration ;
- défense et protection des libertés individuelles par un socle législatif en évolution et la lutte contre la criminalité informatique, alors naissante ;
- accompagnement de la formation à l'informatique dans les écoles, collèges, université.

État et administrations publiques



Peu à peu, les diverses administrations, nationales ou régionales, et entreprises publiques, se sont équipées[1].

On trouvera sur la figure ci-contre, quelques chiffres des investissements correspondants en 2016. De plus, les télédéclarations d'impôts sur le revenu[2] ont connu un vif succès.

[1] la numérisation massive des secteurs : banque, finance, monnaie, bourse, n'est pas évoquée dans ce document.

[2] Le Trésor Public a installé en 2006 un gros système Internet pour les déclarations d'impôt en ligne, pour les Français aussi bien en métropole que dans les territoires d'Outremer. 13 millions de contribuables équipés ont utilisé ce système en 2016, et en 2019, la télédéclaration en ligne sera obligatoire pour tous les contribuables disposant d'une connexion. Une déclaration en ligne documentée pour les revenus de l'année N, suivant sa complexité, prend de 1 à 2 heures. Elle ne nécessite qu'un accès protégé classique (login + mot de passe); comme par le passé, certains éléments de la situation familiale, des revenus salariaux ou de pension, sont préremplis par l'administration. L'intérêt immédiat d'un tel outil est double :

a/ une traçabilité et une réactivité immédiates ;

b/ l'affichage, sans l'utilisation par l'internaute d'un logiciel de simulation, du montant de l'impôt à payer en fin d'année N+1, à l'euro près.

Éducation Nationale

Déjà dans les années 1970-1980, l'Éducation Nationale utilisait beaucoup le Minitel, principalement pour organiser les examens nationaux. Avec Internet, la gestion des moyens de cette administration s'est progressivement numérisée, nationalement et localement.

Par ailleurs, le souci de l'équipement des établissements d'enseignement en matériel numérique (essentiellement, avec des micros connectés à Internet) remonte à une vingtaine d'années. Les chiffres de dotations en matériel, sont en hausse constante. À titre d'exemple, on compte, à la rentrée 2016-2017, 50 % environ de collèges équipés.

Notre Lettre n° 106 détaille quelques aspects du plan numérique lancé en 2017.

Bien entendu, le numérique modifie plusieurs aspects fondamentaux de la vie scolaire : organisation des cours, accès des élèves à toutes sortes de données nationales, usage d'applications pédagogiques simples (histoire, géographie, calcul, apprentissages du français et de l'orthographe...) et, pour les élèves les plus motivés et compétents, apprentissage d'un logiciel.

Santé publique

Notre ami adélien Gilles Trouessin, est consultant senior en Sécurité chez « SRC Solutions ». Il a pleinement exercé la fonction de RSSI dans le domaine hospitalier. Il a animé plusieurs conférences ADELI dans ce domaine.

La sécurité des données médicales a pour fondement, le « secret médical » exprimé dans le Code de la Santé Publique, dont certaines modalités sont précisées dans la Loi Kouchner de mars 2002 :

> *«Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.»*

Entre autres, ce principe entraîne d'importantes contraintes vis-à-vis du « Dossier Médical Personnel » (DMP), en termes de :

- confidentialité des informations ;
- fiabilité, en particulier dans deux domaines :
  - utilisation de la carte interactive VITALE, dans certaines conditions accessibles aux ayants droit de l'assuré ;
  - risque médical lié à d'éventuelles données erronées ;
- protection juridique du dossier médical personnel.

Un des domaines médicaux les plus impactés par le DMP est la cancérologie, par la durée et la complexité des traitements.

Bases de données générales : le « big data » et l'« open data »

Ces deux termes apparus dans les 20 dernières années, couvrent des ensembles de données de même principe, de structures différentes :

- les Big Data (cf. Lettre n° 104) constituent un immense volume de nombre de données (téraoctets soit 10^{12} octets, pica-octets soit 10^{15} octets), issues de tous les traitements en ligne : réseaux sociaux, SMS, mails… Un cas particulier concerne les données commerciales en vue du marketing industriel ;
- les Open Data (cf. Lettre n° 86) désignent des collections de données, qui sont ou devraient être tenues à disposition du public. Elles sont produites ou collectées par un État, une collectivité territoriale, un organe parapublic, dans le cadre de leurs activités au service des usagers.

POLITIQUE PUBLIQUE NUMÉRIQUE : SÉCURITÉ DES SI

Généralités

Dès les débuts de l'informatique, la protection des accès aux données personnelles, professionnelles, publiques, s'est rapidement révélée comme une nécessité, suivant le postulat simple :

> *« Seuls sont habilités à accéder aux données, ceux ayant à en connaître ».*

De cette nécessité ont découlé la formation et la nomination de « Responsables Sécurité du (des) Système(s) d'Information » ou RSSI.

La sécurité des systèmes d'information a pour fondement juridique deux normes décrites dans la Lettre n° 52 : l'ISO 9000, et l'ISO 17991. Aux plans individuel et domestique, la pratique d'internet (et par extension, celle du téléphone mobile), est courante depuis une vingtaine d'années ; et donc, non seulement des outils de protection perfectionnés sont disponibles sur le marché (chiffrement, antivirus, antispam…), mais les comportements des usagers ordinaires ont bien évolué.

Dans l'entreprise, le RSSI a plusieurs fonctions essentielles vis-à-vis des données à accès sensible suivant les 4 critères classiques : disponibilité, intégrité, confidentialité, traçabilité :

- protéger l'informatique interne à l'entité (Intranets de comptabilité, ressources humaines, brevets, décisions managériales, archives numérisées, etc.). Il est souvent secondé par un C(orrespondant) I(nformatique) et L(ibertés), dont le rôle vis-à-vis des fichiers de données personnelles en liaison avec la CNIL, est décrit dans la Lettre n° 73 ;
- sécuriser les éventuelles transactions en ligne avec les clients, en liaison avec les comptes bancaires ;
- former l'ensemble du personnel à des pratiques de sécurité des SI.

Dans les administrations d'État, et également divers secteurs publics (Hôpital, Trésor Public, Police,...), la protection des données sensibles couvre des champs beaucoup plus larges, qu'il s'agisse (cf. notre Lettre n° 102) :

- du domaine militaire et de la sécurité civile, pour les données de protection du territoire (industrie nucléaire, aviation...) et des diverses forces armées ;
- des données individuelles (état civil, dossiers judiciaires, dossiers militaires… - exemples : fichiers STIC et JUDEX) ;
- des informations opérationnelles générales de sécurité : suivi des individus présentant des profils à risques pour l'ordre public ; dossiers des personnes franchissant les frontières dans le cadre des traités de Schengen ; dossiers des passagers aériens ou P(assenger) N(ame) R(ecord). Les attentats de 2015-2016 ont imposé, en particulier en France, une importante refonte du système informatique du renseignement sous toutes ses formes et un accroissement des échanges de données policières et judiciaires, en France et dans l'Union européenne. De même, au printemps 2017, une cyberattaque internationale de grande ampleur vise, dans de nombreux pays, des institutions et administrations sensibles qui, dans un premier temps, instaurent des protections renforcées.
- plus largement, l'application en France, du respect des droits d'auteur dans les transactions en ligne concernant des œuvres artistiques (socles HADOPI et LOPPSI);
- enfin, au plan de l'Union européenne, des démarches volontaristes diverses concernant les GAFA, en particulier la régulation de l'optimisation fiscale des sociétés, ainsi que le respect des libertés individuelles (droit à l'image en particulier) ; ADELI s'en est largement fait l'écho.

Aussi bien dans la sphère publique que dans la sphère industrielle, la fonction de RSSI est confiée à une personne chevronnée, rigoureuse, connaissant bien le domaine de son entité. Compte tenu de

l'enjeu dont elle assure le management, elle est généralement rattachée à la Direction Générale ou locale, suivant la taille de cette entité.

Un organisme central de l'État : l'Agence Nationale pour la Sécurité des Systèmes d'Information

En 2009, une importante Agence d'État, l'ANSSI, forte à ce jour de 400 agents et avec un budget global de 80 millions d'euros, a été directement rattachée aux services du Premier ministre. Ses missions consistent dans la gestion nationale de la sécurité des systèmes d'information, en proposant des mesures et en en vérifiant l'application des mesures adoptées.

Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État.

En outre, elle est chargée de la promotion des technologies, des produits et services de confiance, des systèmes et savoir-faire nationaux auprès des experts comme du grand public : veille générale, développement de produits, information et conseil, formation, labellisation de produits et de prestataires de confiance.

CONCLUSION

Dans ce qui précède, nous n'avons pas évoqué les « emplois nouveaux » générés par les nouvelles technologies. Plusieurs des dernières Lettres, sur le changement y ont été consacrées.

On l'a vu l'État fait - tous gouvernements confondus - de gros efforts pour organiser la modernité technologique, la maîtriser dans le temps, et surtout, en faire partager les fruits par le plus grand nombre. D'aucuns pourraient y voir une tentative d'interventionnisme ; or, nous ne sommes plus, ni dans le cadre d'une économie planifiée des années 1960-1970, ni dans celle d'un libéralisme complètement sauvage et sans règles, malgré le poids international des GAFA.

Pour terminer, constatons une grande similitude entre le monde technologique et celui de la santé : si les progrès techniques enregistrés sont issus de grandes sociétés à pôles Recherche & Développement puissants, le partage des fruits du progrès technique en matière d'entreprise, d'État, de communication et de santé publique, sont des affaires sociétales que chacun doit s'approprier, car chacun est concerné.

RÉFÉRENCES

Ces références sont classées par types et non dans l'ordre d'apparition à l'intérieur du document.

Références générales (principaux liens internet)

- Déclaration de l'expert Olivier Ezratty
- http://www.oezratty.net/wordpress/bio/interviews/

- Discours du Premier ministre L. Jospin (Hourtin, 1999)
- http://www.admiroutes.asso.fr/action/theme/politic/lionel.htmen hyper

- Dépenses de l'État dans les TIC
- https://www.slideshare.net/arturelis/2012-06-18-digital-government-in-france-and-oecd

Références adéliennes : Lettres

- Lettre n° 52 – été 2003 – « l'ISO 9000 de la sécurité »
- http://www.adeli.org/document/396-I52p25pdf

- Lettre numéro 80 – été 2010 – « le rôle du CIL dans l'entreprise »
- https://www.adeli.org/document/532-l80p41pdf

- Lettre numéro 86 – hiver 2012 – « Open Data »
- https://www.adeli.org/document/818-l86p43pdf

- Lettre n° 102 – hiver 2016 - -« Nouvelles technologies, droit et sécurité publique »
- http://www.adeli.org/document/1258-I102p33pdf

- Lettre numéro 104 – été 2016 – « Big Data »
- http://www.adeli.org/document/1297-I297-I104p05pdf