LA SOCIÉTÉ CIVILE FRANÇAISE

LE NUMÉRIQUE EN FRANCE

FRANÇOIS LEMAIRE

Quelques définitions

Par numérique, nous entendons ici l'ensemble des outils qui permettent le traitement automatisé de l'information.

Un point crucial à comprendre pour bien appréhender le numérique est que ces outils sont structurés en couches interagissant les unes avec les autres :

- le matériel :
  - les terminaux (ordinateurs de bureau, téléphones intelligents, tablettes, objets connectés)
  - l'infrastructure réseau (routeurs, équipements réseau filaires et mobiles, grands réseaux de communication, câbles locaux et intercontinentaux, satellites)
  - les serveurs
- le logiciel :
  - le micrologiciel des matériels (plus souvent connu sous le terme anglais de firmware)
  - les pilotes des matériels (ou drivers)
  - les systèmes d'exploitation (pour ordinateur de bureau, mobile, objet connecté ou serveur)
  - les logiciels pour les clients finaux, qu'ils soient locaux ou de plus en plus en ligne
  - les logiciels serveurs
  -

Si on cherche à atteindre le but d'une souverenaité numérique française ou européenne réelle, il s'agit de maîtriser toutes ces couches, ce qui est une tâche dantesque en l'état actuel.

La souveraineté numérique

Le constat

Remontons un peu en arrière, dans les années 70/80. Dans la lignée du plan calcul et du plan "informatique pour tous", la France dispose d'usines de semi-conducteurs et de micro-ordinateurs, crée des systèmes d'exploitation, des logiciels, des équipements réseau, invente le premier service de télématique grand public avec le minitel qui est lui aussi produit en France.

Les enfants de l'époque, dont votre serviteur, sont initiés à l'informatique sur des machines 100 % françaises, Thomson MO5 ou TO7, mises en réseau local dans les écoles. Au début des années 2000, j'ai retrouvé avec une certaine nostalgie quelques-unes de ces vieilles machines dans l'école primaire du village corrézien de 3000 âmes d'où vient ma mère.

A cette époque, la France maîtrise l'ensemble de la chaîne numérique, avec des produits de bonne qualité, pas uniformément parfaits, évidemment. On peut évidemment débattre du modèle français de l'époque, très étatisé - Thomson avait été nationalisé en 1982 et la SIMIV produisant ses ordinateurs fut soutenu à bouts de bras par l'Etat - et du modèle américain fait d'appels d'offres successifs de l'Etat ciblant les entreprises nationales, mais on ne peut nier que la France était alors dans une situation souveraine vis-à-vis du numérique.

Avance rapide en 2021 : nous ne produisons plus de semi-conducteurs pour la micro-informatique, nous ne produisons plus de terminaux grand public, nous ne produisons pratiquement plus de système d'exploitation ou alors confidentiels, nous ne produisons pas d'équipements réseau et encore moins leurs logiciels. Nous avons des entreprises de logiciel client ou de service internet florissantes, mais pratiquement pas de champions mondiaux comme l'est par exemple SAP en Allemagne (il nous reste quelques belles entreprises dans le jeu vidéo). On voit sortir des matériels innovants venant d'entreprises françaises, c'est par exemple Free qui a inventé la "box triple play", mais le travail effectué est un travail d'intégration de composants tiers et de logiciels clients ; la pile complète n'est pas maîtrisée en France ou même en Europe.

Je l'ai vu de près en travaillant à la R&D d'une entreprise française qui produisait ses propres produits de la carte électronique au logiciel client, et qui avait été rachetée par Orange. La stratégie "intégration de composants sur étagère" y a été appliquée de façon bête et méchante, sans tenir compte de la culture d'entreprise. Cette entreprise qui était numéro 1 mondial de son secteur a aujourd'hui été rachetée par le numéro 2 qui est américain... et qui fabrique ses propres matériels.

Bref, nous ne maîtrisons pratiquement plus aucune couche de la pile. Nous sommes entre le marteau américain (systèmes d'exploitation, gouvernance d'internet, services "cloud") et l'enclume asiatique (matériel, micrologiciels). Pire, cette situation est non seulement totalement intégrée par les ingénieurs français, mais aussi considérée comme souhaitable : le choix d'un service cloud américain est considéré comme le choix sûr, le choix qu'on ne peut pas se voir reprocher.

De plus, bien que l'Union Européenne se soit dotée de l'excellent RGPD, et promeuve par là-même un modèle de respect de la vie privée différent de celui des deux autres blocs, la Commission Européenne - et ses donneurs d'ordre les Etats - n'ont de cesse de recréer des accords avec les USA pour continuer à faire fuiter les données personnelles des européens de l'autre côté de l'Atlantique : le Safe Harbor invalidé, elle négociait le Privacy Shield ; celui-ci invalidé en 2020, elle redémarrait de nouvelles négociations aussi sec. A devenir fou !

Notre crédo sur cette question tient en 3 points :

- cette situation n'est pas souhaitable : nous sommes à la merci de l'espionnage américain comme l'ont montré les révélations Snowden, et de l'espionnage chinois, comme l'a montré le scandale Huawei. Nos infrastructure vitales, énergie, défense, communications, médias, appareil productif, dépendent toutes d'un fonctionnement sûr et fiable des outils numériques
- cette situation n'est pas irréversible : nous étions des pionniers, et nous avons des ingénieurs et des chercheurs qui font la fortune des sociétés américaines, coréennes, japonaises. Un seul exemple, mais il y en a des centaines : le chef de la recherche IA de Facebook est Yann Le Cun, un des meilleurs spécialistes français, qui avait obtenu un des premiers résultats technologiques en IA avec le premier OCR
- cette situation nécessite une action vigoureuse à la fois étatique, entrepreneuriale et citoyenne

Le rôle de l'Etat

Il est évident que la pente naturelle actuelle du secteur numérique en France ne va pas dans le sens de la souveraineté. La question du matériel et de son logiciel n'est quasiment plus posée, tout au plus l'affaire Huawei a fait un peu de bruit avant qu'on accorde à SFR un passe-droit pour équiper son réseau 5G en matériel chinois. Les services clouds américains gagnent en permanence du terrain, les DSI se vident au profit de services intégrées. Dernière catastrophe en date : les grandes entreprises se sont jetées dans les bras des outils américains pour le télétravail, Teams de Microsoft fait un véritable malheur. L'Etat lui-même y est assez perméable : il est de notoriété publique que les réunions gouvernementales se font sur Zoom - des journalistes ont même pu s'y inviter en utilisant les failles qui ont été reprochées au service... - l'Education Nationale est une grande amie de Microsoft quand dans ma jeunesse tout le matériel et le logiciel était fabriqué en France, et le Health Data Hub, malgré les recours multiples et les décisions des plus hautes juridictions, prend toujours la direction de Redmond.

L'état de guerre numérique

Nous avons besoin d'un électrochoc venant de l'Etat à destination non seulement du secteur, mais également de la population. Cet électrochoc passerait par la déclaration d'un "état de guerre numérique", qui justifierait la prise des décisions suivantes :

- véto de la France sur toute négociation européenne visant à l'affaiblissement des protections du RGPD
- les services de l'Etat ne pourraient plus, à un horizon de 5 ans, faire appel à des services d'entreprises soumises à une législation moins protectrice que le RGPD, et ce pour toute la pile numérique hors matériel
- les entreprises répondant à des appels d'offre de l'Etat ou des collectivités ne pourraient plus, à un horizon à définir, faire appel à des services d'entreprises soumises à une législation moins protectrice que le RGPD, et ce pour toute la pile numérique hors matériel
- en attendant la mise en oeuvre du point numéro 2, on modifierait les règles des appels d'offre pour que des entreprises respectant ces conditions soient avantagées
- une fois les points 1 et 2 en place, les entreprises pouvant fournir du matériel fabriqué en Europe seraient avantagées dans les appels d'offre de l'Etat et des collectivités. Ces décisions viennent en sus du "Small business act" général.

Cela est d'autant plus possible que c'est une interprétation à peine exagérée d'un des points centraux du RGPD, que l'Etat s'évertue à circonvenir, bien qu'il soit régulièrement condamné par les juridictions !

Il nous semble difficile d'envisager des matériels 100 % fabriqués en Europe à un horizon de court terme. Par contre, des matériels venant d'Asie du Sud-Est mais équipés de micrologiciels et de pilotes Open Source auditables existent déjà.

Etant donné le rôle central de l'Etat dans l'économie en France, l'impact serait massif et immédiat. Les plus grandes entreprises seraient quasiment toutes obligées de mettre en oeuvre des systèmes informatiques souverains.

Garder les chercheurs en France

L'excellent rapport Villani sur l'Intelligence Artificielle traçait la voie vers une Intelligence Artificielle souveraine et maîtrisée. Un de ses points centraux était d'offrir aux chercheurs des opportunités de recherche et des revenus les incitant à rester travailler dans nos universités, nos écoles d'ingénieur et nos entreprises plutôt que de faire remonter le fruit de leur intelligence à Mountain View.

Le jour de la remise de ce rapport, était présent Yann Le Cun, chercheur français débauché par Facebook. Google annonçait financer la chaire d'IA de l'Ecole Polytechnique, qui n'est rien moins que l'école des ingénieurs de l'armée... IBM, Samsung, Facebook annonçaient tous installer des laboratoires d'Intelligence Artificielle en France, utilisant nos informaticiens à leurs propres profits. Bref, le rapport tombait à l'eau le jour même de sa présentation.

Nul n'est besoin de créer une nouvelle commission sur la question : il suffit de réellement appliquer le rapport Villani : créer des postes à l'université sur ces sujets, augmenter la rémunération des chercheurs, leur offrir les opportunités qui feront vibrer leurs neurones.

Aider les entreprises

Comme on le verra dans le chapitre suivant, la commande publique ne couvre pas l'ensemble du numérique, ne serait-ce que les services aux particuliers. Sans déflorer nos propositions au secteur du numérique, nous pouvons déjà dire que l'Etat devrait aider les entreprises françaises et européennes en appliquant strictement le droit européen, et en particulier le RGPD, qui est allégrement bafoué par les acteurs américains comme chinois. Les plaintes auprès d'Apple, Facebook et Microsoft qui ont été lancées par des associations comme la Quadrature du Net traînent misérablement dans les couloirs de la CNIL irlandaise ; la plainte contre Google a donné lieu à une amende d'un montant ridicule par rapport au maximum prévu de 5 % du chiffre d'affaires. Récemment, Facebook a admis qu'une base de données reliant numéro de portable, nom et prénom de la moitié des membres français avait fuité et circulait dans les recoins d'internet, dont ceux de nombreuses personnalités de premier plan, y compris politiques. Pourquoi Mark Zuckerberg a-t-il comparu blême et pour une fois sanglé dans un costume cravate devant la représentation de son pays, et est-il épargné chez nous, voire reçu deux fois comme un hôte de marque, en tête à tête, par notre Président ?

Doper la lutte contre la cybercriminalité

Les 5 dernières années ont vu se développer de manière très importante la cybercriminalité. D'un épiphénomène relativement maîtrisé par une bonne utilisation des outils, elle est passée à une exploitation industrielle par des groupes mafieux de toutes les failles possibles et imaginables, et sur des cibles de plus en plus petites, et donc moins capables de s'en prémunir. Les hôpitaux et les grandes entreprises font assez naturellement la une, mais les PME bloquées pendant des semaines voire perdant à jamais certaines données sont beaucoup plus nombreuses. Pire, les compagnies d'assurance leur conseillent de payer les rançons, ce qui pérennise l'activité des criminels.

Aucun système informatique n'est infaillible ; tout système peut faire l'objet d'intrusion si l'assaillant y consacre suffisamment de temps. Nous devons augmenter drastiquement les effectifs des équipes luttant contre la cybercriminalité, à l'ANSSI, mais aussi dans la police et la gendarmerie. Par exemple, les équipes du BEFTI sont compétentes, mais elles sont en petit nombre, et ne couvrent que Paris et la petite couronne. Avant que quelqu'un ne prenne en charge le dossier, les traces laissées par un éventuel assaillant ne mènent plus nulle part depuis longtemps... Nous proposons de créer des brigades d'intervention rapide spécialisées dans chaque région afin que puissent être recueillies et analysées toutes les informations permettant d'appréhender les criminels.

Par ailleurs, la formation des salariés et du grand public doit être grandement améliorée :

- utilisation des gestionnaires de mot de passe
- utilisation des clés de sécurité et du chiffrement
- sensibilisation au phishing et à l'ingénierie sociale
- importance des sauvegardes et la redondance

Les assurances nous semblent à même d'y prendre leur part, en prévention des attaques plutôt qu'en réparation.

Il va sans dire qu'il est indispensable d'abandonner une bonne fois pour toutes les tentatives par les autorités d'affaiblir les outils de chiffrement. Ils sont la base de la sécurisation des systèmes informatiques, toute porte de derrière introduite pour complaire aux Etats serait exploitée par les cybercriminels.

Suite aux attaques récentes sur des hôpitaux français, notre Président a annoncé le déblocage d'1 milliard d'euros pour aider à la sécurisation des services de santé. C'est un pas dans la bonne direction, mais bien trop timide et limité ; à la fin de la semaine dernière, un opérateur énergétique américain majeur a du arrêter ses opérations à cause d'un rançongiciel, ce qui a fait déclarer l'état d'urgence par le Président Biden. Toutes les infrastructures critiques doivent être examinées et surveillées, pas seulement les services de santé.

Enfin, l'objectif d'une souveraineté numérique participe de cette protection : les révélations Snowden ont prouvé que nos alliés pouvaient nous espionner à l'aide d'outils fournis par leurs entreprises privées, et l'extraterritorialité des lois américaines offre à l'Etat américain et au "Department of Justice" l'accès à des données confidentielles d'entreprises européennes même si le fournisseur héberge en Europe. Par ailleurs, les équipes de cyberguerre chinoises ont réussi début 2021 à exploiter une faille dans Microsoft Exchange afin d'avoir accès pendant près de deux mois aux courriels de milliers d'entreprises américaines, un vrai trésor pour l'espionnage industriel. Un très gros acteur sur lequel sont concentrés des millions de clients est une cible de choix dont une faille devient instantanément une catastrophe, et ce piratage de Microsoft prouve que même les plus grandes entreprises ne sont pas à l'abri de telles mésaventures ; un modèle distribué sur une myriade d'opérateurs de taille moyenne de bonne qualité comme nous le proposons ci-dessous distribue le risque et rend la tâche plus difficile aux assaillants.

Les entreprises du numérique

La stratégie

Bien évidemment, la commande publique ne couvre pas l'entièreté du secteur informatique ; les services au grand public et aux entreprises doivent également devenir souverains.

On peut espérer que la dynamique enclenchée par l'état de guerre numérique gagne les entreprises qui ne seraient pas directement concernées, mais même dans cette hypothèse optimiste, reste la question du grand public, habitué aux services américains que nous connaissons tous, voire chinois comme TikTok.

Là, nous recommandons d'appliquer une page du manuel du parfait petit startuper disruptif. Quand vous arrivez dans un secteur bouché, que ce soit les réseaux sociaux, la fourniture de services de communications électroniques, la vidéo en ligne, etc. la seule façon de pénétrer le marché est de partir sur une proposition de valeur radicalement différente de celles en place.

Les leaders du secteur sont gratuits et se financent sur la vente des données personnelles ? Nous devons fournir des services payants, au moins modérément, ou acceptant les niveaux de revenus inférieurs qui étaient la norme avant la vente du profil des internautes, et respectant strictement le RGPD. Avant 2008, Google avait le modèle d'affaires actuel de Qwant. Aujourd'hui, ils gagnent énormément plus d'argent, mais ils menacent la société. Est-ce ce que nous voulons ?

Les leaders du secteur sont de gigantesques services centralisés qui ne vivent que de la croissance exponentielle ? Nous devons miser sur des services décentralisés, plus résilients, à taille humaine. Cela améliorera également la modération, qui pourra alors être assurée par les gestionnaires de ces services plutôt que par des algorithmes amplifiant les biais de leurs concepteurs, et ralentira la viralité qui peut causer tant de ravages (cf par exemple l'affaire Cambridge Analytica). L'Etat doit aider les entreprises françaises et européennes dans ce domaine en créant l'obligation d'interopérabilité : les services de communication doivent utiliser obligatoirement des protocoles ouverts définis par des organismes indépendants comme le W3C afin de permettre aux utilisateurs de changer facilement de plateforme sans perdre leurs données et leurs contacts. Comme expliqué ci-dessus, quelques centaines d'opérateurs sérieux offrent une surface d'attaque nettement inférieure à deux ou trois services monopolistiques.

Les leaders du secteur et les deux autres blocs, Chine et USA, misent sur la surveillance ? Nous devons l'interdire. Interdiction du profilage automatisé des internautes, des publicités ciblées que ce soit personnellement ou sur des cohortes comme Google le propose avec FLOC, interdiction de la reconnaissance faciale et des autres outils de surveillance automatisée.

Affirmons nos valeurs de respect de la vie privée. Donnons un avantage concurrentiel décisif à nos entreprises dans le monde de Snowden et du crédit social chinois. Nous redeviendrons un modèle de liberté désirable pour le monde entier et un lieu plus sûr pour les citoyens.

Les outils

Arriver aussi rapidement à basculer d'un modèle d'intégrateur et de développement de logiciel à la création d'une pile complète peut sembler insurmontable. En réalité, on constate généralement dans l'industrie informatique le mouvement suivant :

- apparition d'un produit commercial en tout ou partie à sources fermées (aussi appelé "propriétaire")
- le marché arbitre en faveur de ce produit
- le produit devient mature
- des versions logiciels libres sont développées
- au bout d'un certain temps, elles rattrapent en fonctionnalités et utilisabilité leur contrepartie commerciale

Ce modèle n'est pas systématique ; certains outils naissent directement dans le monde du logiciel libre, en particulier quand ils sont issus de la recherche publique, mais ce n'est pas le cas général.

On peut citer par exemple :

- les suites bureautiques : OpenOffice et aujourd'hui leur pendant en ligne comme OnlyOffice sont de qualité similaire à Microsoft Office ou Google Docs
- les systèmes d'exploitation : Linux pour le grand public est aujourd'hui de qualité similaire à Windows et MacOS et est très largement majoritaire sur les serveurs
- de nombreuses bibliothèques de base : openssl fait tourner 95 % de la sécurisation https et est un outil libre qui était maintenu principalement par un brave gars tout seul avant la faille HeartBleed, et que Google considère que c'est un bout de logiciel trop important pour ne pas y mettre un peu de sous (malgré cela, openssl reste un logiciel libre,

Google embrassant ce modèle pour ce qu'il considère comme n'étant pas son coeur de métier)

Ce mouvement se voit aujourd'hui également dans le matériel et les micrologiciels ; quand il y a 10 ans on ne trouvait quasiment aucune machine livrée directement avec Linux, non seulement aujourd'hui les fournisseurs se multiplient, mais depuis quelques années ils proposent au grand public des micrologiciels libres comme coreboot, et même des matériels libres (Pine64, Librem, System76, etc.).

En s'appuyant sur les logiciels, services et matériels libres existants aujourd'hui, on peut rapidement concevoir une pile souveraine pratiquement complète, le matériel restant le point noir, raison pour laquelle nous l'avions exclu de nos propositions sur l'état de guerre numérique.

Cette pile sera-t-elle immédiatement aussi mature et désirable pour le grand public ? On ne va pas se mentir, ce ne sera pas le cas. Raison pour laquelle l'état de guerre numérique et la recherche d'arguments de différenciation par rapport aux logiciels et services leaders sont fondamentaux : à court et moyen terme, la qualité de l'expérience utilisateur sera globalement inférieure. Cependant, en particulier pour ce qui est des outils d'entreprise, nous pensons que l'avantage des logiciels et services américains est largement surévalué. Dans l'industrie, on aurait presque l'impression qu'en dehors de Microsoft ou de Google, point de salut, alors que leur avantage concurrentiel est assez souvent marginal, de l'ordre de quelques pourcents.

Infrastructures de communication

Le constat

Les infrastructures de communication françaises sont dans un état plutôt bon. Nous avons hérité de l'époque des PTT un réseau de téléphonie fixe dense et de bonne qualité, ce qui nous a permis de déployer le haut débit dans tout le pays avec l'ADSL. Toutefois, les caractéristiques techniques de l'ADSL, en particulier la décroissance exponentielle du débit en fonction de la distance au central téléphonique, ont pour conséquence que les débits sont faibles en ruralité, d'où la nécessité d'y déployer la fibre dont le débit et la responsivité dépend peu de la distance.

Le panorama pour le réseau de téléphone mobile est plus contrasté : la couverture 3G est quasiment complète géographiquement, mais la couverture 4G reste concentrée sur les métropoles, les villes moyennes et ce qui leur sert de banlieue. Le démarrage de la 5G se fait par les plus grandes métropoles, on en reparlera. Là aussi, ce sont les zones rurales qui sont à la peine.

La couverture fibre en France est typique des vieux pays d'Europe de l'Ouest ayant un bon réseau de téléphonie fixe ; 65 % des logements sont raccordables, et le taux de raccordement réel est faible. Nous sommes loin des champions asiatiques, la Corée du Sud est à 100 % et le Japon à près de 95 %, et de certains pays qui ont sauté une génération, comme les pays baltes, l'Espagne et le Portugal ou la Russie qui sont tous au-dessus de 90 %. Malgré ce bilan contrasté, nous avons des chiffres bien meilleurs que l'Allemagne, le Royaume-Uni ou l'Italie. Le déploiement de la fibre est fait dans les métropoles par les grands opérateurs ; ailleurs, ce sont les collectivités locales qui sont motrices. Nous en voulons pour exemple le cas du Calvados : Orange a fibré Lisieux, Caen, et leurs banlieues ; le conseil départemental a fibré le reste, atteignant le taux de 100 % de foyers raccordables.

Malheureusement, les grands opérateurs ont refusé d'installer leurs équipements dans les armoires du département, et ont demandé à celui-ci de remettre au pot pour qu'ils daignent mettre la lumière. Le taux d'équipement ne suivant pas, sans doute par méfiance de la population envers les opérateurs de plus petite taille comme K-Net, Kiwi ou Ozone, le conseil département a finalement plié, et paye de la poche des contribuables une modification des armoires qui va plus que doubler le coût initial...

L'insistance de l'Etat à conserver 4 grands opérateurs nationaux, et éviter de descendre à 3 où un oligopole se mettrait très probablement en place (on a encore en mémoire le "cartel du SMS", où les 3 opérateurs de l'époque s'étaient entendus pour conserver des prix publics délirants pour les SMS par rapport au prix de revient), permet d'une part un bon niveau d'innovation technique - Free est par exemple l'inventeur mondial de la "Box Triple Play" - et un niveau de prix assez bas, et ce contrairement à ce qu'Arnaud Montebourg craignait en son temps de Ministre du Redressement Productif, sans impacter la capacité de nos opérateurs à continuer d'investir dans les réseaux. ###

La question de la 5G

La question de la 5G Le débat sur la 5G a fait rage et continuera à faire rage pour les années à venir. Il est dominé par une polarisation manichéenne entre de supposés amish complotistes coiffés de chapeaux en aluminium et des turbo transhumanistes lancés à la poursuite du futur. Comme toujours, la vérité sur la question nous semble plus complexe.

La 5G, comme 5ème génération, n'est pas une technologie unique, mais un ensemble de technologies qui seront mises en œuvre petit à petit et avec des objectifs bien distincts. Les fréquences que l'Etat a vendues à l'automne 2020, et qui constituent le démarrage national de la 5G, sont des fréquences similaires à celles utilisées pour la 4G ; d'ailleurs, beaucoup d'antennes n'ont pas besoin d'être modifiées pour les utiliser, une mise à jour système peut suffire. Sans rentrer dans les détails techniques, cette première phase du déploiement de la 5G apporte trois améliorations, que nous classons par ordre décroissant d'intérêt :

- une portée plus longue des ondes, ce qui en théorie nécessiterait moins d'antennes pour couvrir les zones rurales
- un mode veille pour les équipements, ce qui théoriquement devrait réduire la consommation énergétique
- un débit plus important

Ces fréquences sont légèrement plus énergétiques que celles de la 4G, les antennes consommeront donc en fonctionnement plus que les antennes 4G ; cependant, théoriquement, la puissance nécessaire à l'octet transmis est inférieure. Il est ici intéressant de mentionner une étude de l'Ademe de fin 2019 sur la consommation électrique à l'octet des principales technologies pour accéder à internet : la fibre est la championne de la sobriété, et de loin ; l'ADSL consomme environ 4 fois plus d'électricité à l'octet, et la 4G dix fois plus. Même si les économies théoriques de la 5G issues du mode veille et de la plus grande efficacité de ses fréquences venaient à devenir réalité, elle resterait au moins 3 fois plus consommatrice à l'octet que la fibre et serait peu ou prou équivalente à l'ADSL.

Le deuxième étage de la fusée 5G met en œuvre des ondes d'une fréquence bien supérieure à celle de la 4G et de la 5G "v1". L'intérêt de ces fréquences très élevées est de grandement améliorer le ping de la connexion pour atteindre la qualité d'un ping de fibre, c'est-à-dire sa réactivité, et de permettre de multiplier les terminaux. Le défaut est que ces ondes ayant une longueur d'ondes très petite (la longueur d'onde est l'inverse de la fréquence), elles sont très sensibles aux perturbations, et pénètrent très peu les obstacles. A tel point qu'on réfléchit à créer des matériaux pour les bâtiments, en particulier les fenêtres, spéciaux pour que les ondes 5G haute fréquence puissent passer. Par ailleurs, cette sensibilité aux perturbations implique que le nombre d'antennes doit être très élevé, de l'ordre d'une antenne tous les 200 mètres. On imagine aisément qu'une telle densité d'antennes est peu envisageable dans les zones rurales, où installer une antenne tous les 4 ou 5km est la norme.

Les promoteurs de cette 5G dense la considèrent nécessaire pour les applications suivantes :

- l'inoxydable vendeur de technologies internet qu'est la chirurgie à distance. Cette fonctionnalité m'avait déjà été présentée comme un point fort de l'ADSL en 1996 en école d'ingénieur... Outre le fait que la chirurgie à distance se fait avec la fibre depuis près de 15 ans, on voit mal un chirurgien opérer en mobilité, en faisant son footing ou en voiture.
- la multiplication des objets connectés : aujourd'hui, les objets connectés envoient leurs données soit en utilisant des ondes radio basse fréquence (pour des objets éloignés de toute connexion internet et nécessitant peu de débit), soit avec des clés 3G (si un débit important est nécessaire, mais la consommation électrique est très élevée) ou par un wifi local. La 5G "dense" avec son mode veille limiterait la consommation électrique, aurait la capacité d’accommoder un nombre bien plus élevé d'objets, tout en nécessitant 0 configuration, ce qui est le défaut du wifi. Il est à noter cependant que le mode veille des antennes qui est un point central de la supposée consommation plus basse de la 5G serait probablement peu activé si un grand nombre d'objets connectés se retrouvaient à émettre régulièrement autour de celles-ci ; ce mode veille ne concernerait alors que les terminaux. Ceux-ci constituant plus de 45 % de la consommation, le gain serait tout de même notable.

- la voiture autonome : d'une part, le ping de connexion est vital pour un dispositif qui a des décisions de vie ou de mort à prendre ; d'autre part, il est probable que pour atteindre le plein potentiel des voitures autonomes, de très nombreux objets connectés à connexion rapide et fiable soient nécessaires

- les éternelles applications auxquelles on n'a pas encore pensé, et sur lesquelles il est difficile de baser sa réflexion, à moins de poser une pétition de principe que toute nouvelle technologie est souhaitable, ce qui n'est pas notre avis comme vous l'aurez compris

Pour en terminer sur cette présentation de la 5G, il est intéressant de noter que quelques pays ont déployé la 5G depuis quelques mois avec les résultats suivants :

- tout le territoire de Monaco est couvert de 5G : les pompiers monégasques notent de meilleures images de leurs drones de surveillance, le débit est effectivement amélioré. Et... c'est tout.

- la Corée du Sud et le Japon font état d'un débit amélioré

- la Chine a déployé quelques zones en 5G dense : un port connecté entièrement autonome, sans dockers, et quelques quartiers de grandes villes. Dans ces derniers, les opérateurs ont forcé le mode veille de façon assez agressive car la consommation électrique s'envolait.

Malheureusement, nous n'avons pas trouvé d'étude aussi poussée que celle de l'Ademe sur la consommation électrique. Gageons qu'elles ne devraient pas tarder à apparaître, même les pays les plus techno-optimistes se préoccupant de ces questions.

Enfin, en France, bien que le principal apport de la 5G "v1" soit de faciliter la couverture de zones rurales, les premiers déploiements sont effectués par les opérateurs dans de grandes métropoles, et pour cause, c'est là qu'il y a le plus de clients. Et les publicités d'annoncer que les heureux possesseurs de forfaits 5G pourront regarder des vidéos en 4K à la fin de leur footing sur leur téléphone intelligent. Quand on voit la taille de l'écran, on se dit qu'y visionner une vidéo en 4K est vraiment essentiel ! Les débuts de la commercialisation de la 5G, et le peu de contenu probant des publicités,

Nos propositions pour la France

Les gains procurés par une 5G déployée sur tout le territoire sont discutables :

- une réduction de consommation électrique non prouvée par le peu de retours d'expérience que nous avons

- la capacité à déployer de très nombreux objets connectés envoyant des données à très haut débit : outre le fait que cela remettrait en cause les économies potentielles, on a du mal à voir l'usage du très haut débit pour ces objets, à part pour la surveillance dont nous sommes peu friands

- des déploiements facilités en ruralité, zones qui ne disposent déjà pas de la 4G et ne sont pas du tout dans les plans des opérateurs pour la 5G

A notre avis, il est urgent d'attendre sur ce dossier, le gouvernement aurait été bien inspiré de ne pas vendre les fréquences nationalement et d'autoriser uniquement une expérimentation grandeur nature, par exemple dans une métropole et un département rural, afin de vérifier si les gains réels justifient un investissement aussi massif. Il a sans doute été séduit d'une part par l'affichage technologique que constitue le début de déploiement de la 5G, et d'autre part par la manne financière provenant de la vente de ces fréquences...

Il nous semble à l'opposé absolument vital d'accélérer le déploiement de la fibre pour atteindre les chiffres des pays les plus avancés en la matière ; c'est la technologie la plus performante, la moins consommatrice d'énergie, et la plus pérenne pour accéder à internet. Les gains sont connus depuis près de 15 ans, et les collectivités locales, les plus au fait des besoins de leurs administrés, ne s'y sont pas trompées. Il nous semble que l'Etat est beaucoup trop complaisant auprès des grands opérateurs nationaux ; la transformation du plan fibre en plan Très Haut Débit leur permet de remplacer des déploiements fibre par des déploiements mobile ce qui risque d'aboutir à un taux final nettement en deçà des 90 %. Nous proposons de revenir à un plan fibre visant les 95 % de raccordabilité et de rendre cet objectif contraignant pour les opérateurs nationaux.

Enfin, pour revenir sur l'aspect souveraineté, l'exception accordée à SFR sur les équipements Huawei pour la 5G nous semble problématique. Une fois le réseau installé et configuré pour plusieurs années, SFR fera-t-elle l'effort de le revoir de fond en comble, ou l'exception sera-t-elle renouvelée ad vitam æternam ?

Le numérique et l'Etat

Accélérer sur l'OpenData

La France a voté plusieurs lois consacrant l'OpenData, c'est-à-dire la mise à disposition aux citoyens, aux associations et aux entreprises des données créées par les administrations. Malheureusement, les contraintes sont notoirement insuffisantes, et il n'est pas rare d'attendre des mois que la CADA accède à des demandes de fourniture de documents. L'OpenData reste aujourd'hui de facto à la discrétion des administrations ; certaines sont très volontaires, comme le ministère de l'agriculture, et d'autres traînent des pieds voire refusent purement et simplement - ce qui est illégal, rappelons-le - comme le ministère de l'intérieur. Or l'OpenData n'est pas une simple lubie de militant ; nous en voulons pour preuve le travail de Guillaume Rozier pendant la crise du COVID-19 avec son site CovidTracker. Avec ses équipes, il a collationné des informations publiques disparates sur l'épidémie, et en les combinant a créé des statistiques utilisées par le gouvernement lui-même. Ces derniers mois, il a également créé le site vitemadose qui est un "mashup" des différents services de réservation de rendez-vous de vaccination. Pas que l'Etat ne pourrait pas lui-même créer ces services, mais ses ressources sont limitées, et plus nombreux sont les esprits se penchant sur un problème, plus la probabilité de trouver une solution augmente.

La loi pour une République Numérique de 2016 a en grande partie amélioré la situation, bien qu'ayant rajouté certaines exceptions sur la mise à disposition des codes sources pouvant mettre en danger la sécurité des systèmes d'information de l'Etat, ignorant par là-même la longue expérience accumulée par les informaticiens sur le fait que les logiciels à sources ouvertes ne sont ni plus, ni moins attaquables que les logiciels propriétaires. Elle institue une autre limitation en ne comprenant pas les documents non créés sous forme numérique ; par exemple, le code source de Parcoursup a été publié, mais le gros de la décision est prise lors de commissions dans les divers établissements d'enseignement supérieur. Nous n'avons aucune information sur ces commissions, quels critères y sont appliqués, si elles utilisent des méthodes algorithmiques ou une évaluation informelle orale du dossier de chaque étudiant. L'administré n'est pas très avancé.

Nous proposons qu'à l'instar du DPO institué par le RGPD, on crée un référent OpenData dans chaque structure identifiée par la loi comme productrice de données à caractère public. Tout comme le DPO, ce responsable OpenData aura la tâche de cartographier les données à publier, de promouvoir en interne l'OpenData et sera responsable de sa mise en œuvre. Par ailleurs, le parcours pour un administré se voyant refuser l'accès à une donnée est trop long, la CADA dépassant allègrement le délai légal de 30 jours pour fournir sa réponse. Nous proposons d'une part d'augmenter les moyens de la CADA, et qu'à défaut d'une réponse dans les 30 jours, la requête soit de fait accordée comme cela est déjà le cas pour de nombreuses demandes administratives. ###

Numérisation des services de l'Etat

L'Etat français a en grande partie rattrapé son retard sur les services en ligne par rapport aux pays les plus avancés. Cependant, il a trop souvent utilisé la mise en place de services en ligne pour fermer des services physiques, or d'après une étude de l'INSEE de 2019, l'illectronisme touche 17 % de la population ; 25 % ne savent pas s'informer, 20 % ne savent pas communiquer par internet et 12 % n'ont pas du tout d'accès à internet à disposition. Les personnes les plus touchées par l'illectronisme ou le manque de matériel sont des personnes déjà en difficulté par ailleurs, difficultés sociales, niveau d'éducation plus faible, difficultés cognitives dues à l'âge ou au handicap. Il en résulte une perte de chance supplémentaire et une restriction de l'accès aux services publics qui mettent à mal nos principes de solidarité et de fraternité. Il nous apparaît crucial que les économies effectuées grâce aux services en ligne de l'Etat servent à ce que chaque service numérique soit doublé par un service physique à destination de ces publics.