Pourquoi il faut fermer Euratechnologies

Contre la cybersécurité et notre cybervie

Dans une Europe en crise, l'économie de la région Nord-Pas de Calais est moribonde. Les taux de chômage, de cancers, de pollution, de suicides, d'alcoolisme ou d'incarcération disputent les premières places – principalement à la Haute Normandie et à l'Île de France.
Ses dirigeants, élus et industriels, n'en finissent plus de nourrir l'illusion d'une « redynamisation du territoire » et la promesse de nouveaux saccages : agrandissement des ports de Calais et Boulogne, développement de l'aquaculture, du tourisme, saignée du canal Seine-Nord, construction d'un grand stade, projets de trams-trains, de centrales à gaz, d'énergies renouvelables. On rase les friches industrielles et urbaines pour bâtir les friches de demain. Voir la Zone de l'Union, par exemple. On greffe un Louvre à Lens en espérant qu'il soit un « levier » de croissance pour le bassin minier – tout en saluant, des trémolos dans la voix, le courage de ces générations de silicosés sacrifiés pour la France. Surtout, on mise sur la « Recherche & Développement », activité première et centrale pour ouvrir des perspectives de profits et d'emplois. Principalement dans l'économie numérique, le nouvel eldorado industriel de ce début de siècle.

Nous avons déjà détaillé les projets numériques de la métropole lilloise.[1] Le plus intrusif s'appelle U-City, pour ville « ubiquitaire » : six millions d'euros alignés pour moitié par l'État (3 Millions), l'Europe (1,5 M), la Région (800 000), Lille Métropole (800 000) et des fonds privés. Il commence avec Éric Quiquet, la carte RFID « Pass-Pass » et les téléphones portables pour payer les transports en commun et alimenter un fichier des déplacements. À terme, cette carte, ou le téléphone équipé de l'application adéquate, sera nécessaire pour payer la piscine, la cantine scolaire, les musées, les commerces, emprunter des livres à la bibliothèque et s'inscrire aux services sociaux. Le Pôle des industries du commerce (PICOM-Auchan, hébergé par Euratechnologies) travaille à géolocaliser les propriétaires de téléphones, les guider vers les enseignes partenaires et leur envoyer des publicités ciblées. C'est annoncé dans une délibération métropolitaine du 14 décembre 2012.[2]

Depuis octobre 2012, Cédric Hozanne, directeur général de Natural Security hébergé par Euratechnologies également, a installé des lecteurs biométriques aux caisses du supermarché Auchan de Villeneuve d'Ascq. L'empreinte veineuse des doigts remplace le code bancaire. Une carte RFID détectant le client à proximité de la borne remplace la carte bleue. Passée la phase expérimentale, l'identification biométrique se généralisera jusqu'aux distributeurs de billets.

Parmi les organisateurs de cette ville « intelligente » ou *smart city* ou ville « ubiquitaire », à laquelle chaque Nordiste accédera avec sa « carte de vie quotidienne », on trouve Chekib Gharbi, directeur du Centre d'Innovation des Technologies sans Contact-EuraRFID (CITC-EuraRFID, sis à Euratechnologies). Il énonce ses velléités comme tel : « *l'identification, la traçabilité, la mobilité, la localisation, la sécurité et la sûreté* » des citadins lillois.[3] Il nous aura prévenu. En nous dotant de cartes d'identité électroniques indispensables à la moindre interaction sociale, Lille Métropole et le Conseil régional nous transforment en stocks, en flux, en algorithmes gérés à distance. Nous devenons des humains « augmentés », des piétons « augmentés », des consommateurs « augmentés ». D'une part, les relations humaines se transforment en

1 Voir *L'Enfer Vert*, tomjo, Badaboum, 2011.
2 Convention avec la caisse des dépôts pour le financement du projet U-City au titre des investissements d'avenir, délibération du 14 décembre 2012, Lille Métropole.
3 sanscontact.wordpress.com

« interconnexions » *via* des supports technologiques. D'autre part, c'est avec notre environnement que nous « communiquons » technologiquement : on appelle ça les interactions hommes-machines.

Par exemple, depuis janvier 2013, Euratechnologies pilote le projet européen « smartculture ». Goûtez la prose du Conseil régional à ce sujet : il s'agit de renforcer la recherche et l'innovation « *au sein du secteur culturel et créatif pour améliorer les usages et les applications numériques dans le domaine du patrimoine culturel numérique, des réseaux sociaux, et des "smartculture".* »[4] Si A = A alors A = A. Et inversement. Ou comment développer des outils dans l'espoir de développer d'autres outils, mais sans jamais se demander pour quoi. Art numérique et numérisation des œuvres, voilà le projet.

La « *nordist touch* », ça vous dit quelque chose ? C'est le nom donné à la région pour son volontarisme dans les « univers virtuels » et les *serious games*, ces jeux vidéo pédagogiques à visée militaire et industrielle.[5] Les têtes de gondole sont les entreprises Ankama, sur la Plaine Images de Roubaix, et V-Cult basée à Euratechnologies. En plus de travailler huit heures par jour devant un écran, celui-ci s'accapare déjà la moitié de notre temps de loisirs – télévision ou ordi. Quatre heures de télé contre 18 minutes de lecture par jour[6], c'est encore trop de livres pour Euratechnologies. La moitié de notre temps libre devant un écran, c'est encore trop de relations humaines. Vitrines tactiles, publicités intelligentes qui identifient les passants (projets PICOM), un filtre virtuel s'interpose entre nous et la réalité pour nous imposer un monde d'artifices.

Troisième étape : après le puçage du bétail humain pour interagir avec ses pairs puis son environnement, les divers capteurs coloniseront un espace dans lequel les objets communiqueront entre eux pour se gérer d'eux-mêmes. « *La région usine de la France devient hyperbranchée et décomplexée sur les usages numériques, les espaces urbains connectés ou la ville durable. Pierre de Saintignon, premier vice-président de Région au développement économique rappelle "les grandes ambitions sur l'Internet des objets", tout ce qui connecte les objets entre eux.* »[7]

Pour continuer de nommer ces malfaiteurs vautrés dans l'assistanat grâce aux aides publiques déversées depuis l'Europe jusqu'à la métropole, notez qu'ils sont regroupés derrière Raouti Chehih, le directeur d'Euratechnologies. La région héberge aujourd'hui 1 500 entreprises et 24 000 salariés travaillant pour le développement du numérique. Dont 1 500 uniquement à Euratechnologies. Le filon est trouvé, les élus ne vont pas en rester là. Dans son Programme stratégique 2014-2020, le Conseil régional prévoit un Observatoire des communications électroniques et des projets d'e-administration, de télé-apprentissage *via* une université numérique, d'Internet de l'énergie, de télé-médecine (consultations et soins par Internet), de domotique pour les personnes dépendantes (logements automatisés, munis de capteurs et reliés à Internet). Pour ce faire, la Région ouvrira un pôle d'excellence dédié à l'Habitat et aux bâtiments intelligents afin de sceller notre dépendance à ces béquilles technologiques sans lesquelles nous ne pourrons plus faire nos courses, cuisiner, nous chauffer, discuter, apprendre, nous rencontrer, respirer. Le bailleur Lille Métropole Habitat mettra en place des *smart system* dédiés au logement social. Cela va sans dire : c'est une question de développement durable.

Remonté comme un coucou, Pierre de Saintignon nourrit des prétentions grandiloquentes : « *L'élu revient de cinq jours de voyage en Chine avec Luc Doublet, président de CCI International, pour plaider à Pékin, Shanghai et Shenzhen la cause d'une présence des grandes signatures numériques chinoises à Lille. "Nous sommes revenus avec une corbeille pleine", a-t-il confié.*

4 « Diagnostic territorial stratégique - Programmes européens 2014-2020 », Conseil Régional Nord-Pas de Calais.
5 « Des jeux vidéo pour une contrainte ludique », labrique.net, juillet 2012.
6 Source : Médiamétrie.
7 lavoixeco.com, 23 novembre, 2012.

Verra-t-on un jour le concurrent direct de Google s'installer à Lille aux côtés des équipes d'Ericsson, leader mondial et suédois des réseaux intelligents, prospectés en septembre à Stockholm avec le comité Grand Lille ? » s'impatiente *La Voix du Nord*.[8] Le 22 novembre 2012, Aubry, Saintignon et Chehi, le directeur d'Euratechnologies, ont reçu les encouragements de la ministre de l'Innovation et du Numérique Fleur Pellerin pour leurs projets de quadrillage numérique du territoire : « *La Région votera le 13 février son plan sur le très haut débit, le campus de l'innovation prend forme à Euratechnologies, et avant de visiter une maison du futur conçue par un centre des technologies sans contact sans équivalent en province, la ministre put exprimer son souhait de voir une collectivité de la région se porter candidate au test d'un "territoire intelligent grandeur nature, avec d'importants soutiens financiers", rappelant que le très haut débit pour tous les Français d'ici dix ans était le quatrième engagement du candidat Hollande.* » Qui seront les cobayes de ce « *territoire intelligent* » grandeur nature ? Les Lillois ? Les Villeneuvois ? Les Roubaisiens ? Avec son Schéma d'aménagement numérique voté en juillet 2011, Lille Métropole a pris de l'avance et installe la fibre optique nécessaire à supporter les gigaoctets qu'enverront les capteurs et les caméras haute définition dans les tuyaux de l'information.

Cette « *maison du futur* » qu'a visitée la ministre Pellerin est emmenée par un certain Isam Shahrour de l'université Lille 1 et se nomme Sunrise – *Smart Urban Networks for Resilient Infrastructures and Sustainable Ecosystems*.[9] Un site dédié à la gestion de l'eau et de l'électricité, et à la prévention des risques : « *défaillance de fourniture d'eau et d'énergie, contamination des ressources, inondations, effondrement, sécheresse,..)* » Les capteurs installés sur le réseau calculeront en temps réel la qualité biologique et chimique de l'eau, la température, surveilleront la consommation et les défaillances du système pour une transmission automatique des informations auprès des consommateurs et des équipes de maintenance. Avec les compteurs intelligents *Linky*, il en sera de même pour l'électricité.
La mobilisation est presque totale pour mener ce projet. Il ne manque que les « usagers ». Le laboratoire de recherche comprend Lille 1, le plus grand institut de recherche dans la sécurité des réseaux d'eau W-Smart, le Commissariat à l'énergie atomique et KWR, une agence de consultants. Parmi les « opérateurs » se trouvent IBM, la multinationale de la planète intelligente, Suez et Véolia pour l'eau, et ERDF pour les réseaux électriques. « *Dans un contexte d'urbanisation importante, les questions de la raréfaction des ressources énergétiques, de l'augmentation des gaz à effet de serre, de l'envolée des coûts liés au traitement de l'eau et des déchets, de la santé humaine* » se résoudront par une fuite en avant dans le contrôle et l'automatisation (note de presse CITC, Lille 1, Eaux du Nord, 26 février 2012). Mieux vaut sacrifier notre liberté que la cause des « dysfonctionnements » : notre modèle technique et urbain qu'ils s'acharnent à développer.

Carte de vie quotidienne pour les humains, interactions hommes-machines, et finalement environnement autonome, c'est ça une *smart city* : la dépossession de nos vies. Si vous n'êtes pas convaincus de cette ville assistée par ordinateur, vous vous ferez bourrer le mou dans des opérations de propagande telles que le dernier Café métropolitain organisé en septembre 2012 par Lille Métropole et Euratechnologies sur « *La ville du futur et vous* ». Ainsi que par des expos artistico-numériques dont Lille 3000 a le secret.

La cybersécurité de notre cybervie

« *Aujourd'hui un virus informatique peut s'attaquer à une centrale nucléaire, à un barrage, à notre réseau de transports, faire dérailler un train ou attaquer la Banque centrale. Avec l'interconnexion, on peut mettre en l'air toute l'organisation sociale* » a-t-on entendu au

8 *Idem*.
9 sunrise-lille.fr

Forum international de la cybersécurité (FIC) à Lille Grand Palais les 28 et 29 janvier 2013. 2 400 professionnels, 48 conférences, et trois ministres dont Manuel Valls venu clôturer ces deux jours. Cette sauterie voulue par Pierre de Saintignon était organisée par la gendarmerie nationale, le Conseil régional et le Centre européen d'intelligence stratégique. Euratechnologies étant la « *cheville ouvrière* » de l'événement. Toutes les forces de l'ordre étaient représentées : l'Imprimerie nationale, la Délégation générale à l'armement, Alcatel-Lucent, l'Agence nationale de sécurité des systèmes d'information (ANSSI), l'OTAN, le fabricant de supercalculateurs Bull, Cassidian Cybersecurity – filiale sécurité du fabricant d'armes aérospatiales EADS –, Orange, Google, La Poste, la SNCF, EuraRFID, Thalès, des écoles d'ingénieur, etc. Toutes ces entreprises vendent ou ont besoin de cybersécurité. Sous leur impulsion, notre monde toujours plus connecté est toujours plus en proie aux menaces cybernétiques. Ces entreprises ont les solutions aux défaillances techniques et aux cyberattaques auxquelles elles se soumettent elles-mêmes. La boucle est ainsi bouclée. Elles gagnent à chaque étape. Et notre histoire se referme dans une dépendance accrue envers leurs compétences techniques.

« *On ne peut pas parler de développement technologique sans parler de la protection des données* », *dixit* Saintignon. C'est une question de « *confiance numérique* ». Ce n'est pas un hasard si ce forum international s'est déroulé à Lille. Volontaire dans l'édification de la « ville intelligente », la Région inaugurera en septembre 2013 un cluster (pôle d'excellence en techno-français) « *qui fédérera les acteurs de la cybersécurité, les universitaires, les centres de recherche, les acteurs publics... tout cela au service des entreprises basées à Euratechnologies. […] La création de ce cluster, c'est un véritable message économique et, vu de Chine, ça a de l'allure !* »[10] Vu depuis le commun des mortels, ça n'a aucun intérêt. Mais Saintignon ambitionne de faire de Lille « *la capitale européenne et mondiale de la cybersécurité.* »[11] Excusez du peu.

Panorama de la course à l'armement numérique. Le Pentagone vient d'annoncer qu'il multiplierait par cinq ses effectifs voués à la cybersécurité.[12] Comme on l'a constaté auprès des industriels et militaires réunis durant ce FIC 2013, les attaques des virus américains *Flame* et *Stuxnet* sur les installations nucléaires iraniennes en 2009 ont eu l'effet d'une bombe. Tannés d'un côté par Israël pour lancer une attaque contre la République atomique d'Iran, mais embourbés de l'autre dans une situation afghane qui rendrait toute nouvelle opération militaire impopulaire, les États-Unis concédèrent une attaque informatique secrète contre les installations nucléaires iraniennes. Obama, premier pirate du net. Les virus, mis au point pour endommager les systèmes informatiques de Siemens installés en Iran ont détraqué mille centrifugeuses d'uranium et retardé de plusieurs mois le programme nucléaire. À l'aide d'une simple clé USB. Judicieuses, ces attaques informatiques sortent de toute réglementation internationale. Même si les virus ont le même effet que plusieurs kilos d'explosifs pour endommager des sites sensibles, les États-unis ne sont pas officiellement en guerre. Mais si d'aventure une attaque cybernétique s'en prenait à leurs intérêts vitaux, les États-unis ont prévenu qu'ils riposteraient avec des armes conventionnelles.

Depuis l'épisode iranien, la France redouble d'effort pour s'équiper en moyens de défense numérique. « *Comment la France doit-elle faire pour se préparer contre un cyber 11 septembre ?* », s'alarme le député Edouardo Rihan Cypel pendant une conférence du FIC. Le prochain Livre blanc sur la sécurité et la défense nationale du président Hollande promet de faire la part belle aux questions cybernétiques. Et le ministre délégué aux anciens combattants Kader Arif assure que le financement des recherches consacrées à la cyberdéfense, *via* la Délégation générale à l'armement (DGA), « *a doublé cette année et atteindra à court terme 30 à 35 millions d'euros par an.* » Budget qui aura triplé en quelques années. Des filières universitaires s'ouvrent à la hâte pour former des ingénieurs en sécurité des réseaux. L'école militaire Saint-Cyr a ouvert

10 *La Voix du Nord*, 28 janvier 2013.
11 fic2013.com
12 lemonde.fr, 28 janvier 2013.

une formation. La DGA et l'École des transmissions ouvrent un pôle d'excellence en Bretagne. Et une filière « cybersécurité » se met en place à l'université Bretagne-sud. Les industriels, quant à eux, ont aussi leurs réponses : Cassidian cybersecurity (EADS) et Thalès réservent 20 % de leur budget de « Recherche & Développement » à la sécurité informatique.
Du fait du caractère militaire *et* civil des attaques cybernétiques, « *l'état-major des armées a souhaité mettre en place un réseau de réservistes spécialisés en cyberdéfense dans le cadre de la réserve citoyenne.* »[13] Les cyberflics se multiplient. Et soyons sûrs que la sensibilisation de la nation – étudiants, chercheurs, journalistes, citoyens – à la défense numérique sera assurée lors des prochains Cafés défense que mène la Mission Lille eurométropole défense sécurité.[14]

La cybervie quotidienne comme la cybersécurité sont des secteurs économiques en pleine croissance. Peut-être même que la réalité des menaces est surévaluée tellement les perspectives de gains sont grands pour nos cybermaîtres : le cabinet d'audit PwC prévoit « *un rythme de croissance de 10 % par an d'ici au milieu de la décennie, par rapport à un marché mondial de quelque 60 milliards de dollars en 2011.* »[15] Edouardo Rihan Cypel y met tous ses espoirs pour répondre au marasme économique : « *Lorsque nous traversons une crise économique sans précédent depuis les années trente, une crise qui est aussi une mutation économique, une réorganisation du mode de production, une révolution industrielle liée au numérique, il y a une opportunité pour la France de créer une nouvelle filière économique et industrielle à même d'apporter un nouveau cycle de richesses et de croissance. La France doit être à l'avant-garde de la* bataille *économique qui se joue du point de vue du cyber* »[16] (FIC 2013). Thalès, Safran, Morpho, EADS, Bull, ces industries françaises encore « *trop dispersés* » d'après Fleur Pellerin, devront travailler ensemble pour atteindre cette « masse critique » qui positionnerait la France sur le marché mondial. C'est toute l'ambition d'un cluster régional tel que celui de Pierre de Saintignon. Il « *fédérer[a] l'ensemble des énergies et des acteurs régionaux* » pour relancer la machine économique régionale et gagner la confiance des entreprises multinationales. Chercheurs, grande distribution, urbanistes, gestionnaires, élus, industries du transport et du numérique, etc. D'ores et déjà, l'entreprise villeneuvoise de cybersécurité Netasq (EADS) a signé un partenariat avec l'école d'ingénieurs Telecom Lille 1 pour préparer les étudiants en Sécurité des réseaux et des systèmes « *à entrer dans la vie active encore mieux armés.* »[17]

Armés contre qui ?

De façon générale : « *Un certain nombre de problèmes relèvent en même temps des questions de défense et des questions de sécurité. On était dans un système binaire : oui-non, guerre-paix, civil-militaire. Et progressivement on a abouti à un système où à chaque situation de crise doit correspondre une combinaison d'actions et de moyens dosés en fonction de la nature de la crise* » (Général de gendarmerie Wattin-Augouard, FIC 2013). Exemples : la piraterie maritime ou le narcotrafic international, menaces non gouvernementales, appellent cependant une réponse militaire. Tel est le cas également sur Internet. Le *continuum* défense-sécurité.

La prévention des cybermenaces s'explique par la nécessité de garantir la souveraineté industrielle nationale : « *Si la France veut être influente, il faut qu'elle ait la capacité de protéger ses secrets, qu'ils soient étatiques, scientifiques ou économiques* », déclarait Guillaume Poupard, responsable du pôle « sécurité des systèmes d'information » à la DGA. Une question de « *confiance numérique* », dirait Saintignon. Avec la multiplication des supports de communication tels que les

13 « La montée en puissance de la cyberdéfense au sein des armées », A. Coustillière et M. Gallant, *Revue de la Gendarmerie nationale* n°244, décembre 2012.
14 « Renforcer le lien recherche – défense – nation. L'exemple des nanotechnologies », hors-sol, décembre 2012.
15 *Reuters*, 28 janvier 2013.
16 C'est nous qui soulignons.
17 Communiqué de presse Netasq-Telecom Lille 1, 27 novembre 2012.

tablettes et les smartphones, la 3G et maintenant la 4G, ou le *cloud* (conservation délocalisée de données numériques), l'espionnage industriel et militaire s'intensifie. Les événements d'« extraction de données » affectent les industries dans la course technologique qu'elles se mènent. « *Les systèmes informatiques des institutions et des entreprises américaines sont les cibles régulières et récurrentes de cyberattaques qui mettent en péril la compétitivité économique des États-Unis* » s'inquiète *Le Monde* du 11 février 2013. Les principales attaques proviendraient de la Chine qui s'est faite une spécialité du cyberespionnage. Les secteurs les plus attaqués étant « *l'énergie, la finance, l'aérospatiale et l'automobile [...]. Les dommages causés par ces attaques sont estimés à des dizaines de milliards de dollars.* » Les secrets industriels civils et militaires, moteurs de croissance et de puissance, seront protégés par la DGA.

Le matin du forum, le 7/9 de *France Inter* annonce l'événement en agitant l'épouvantail des pédophiles sévissant sur Internet et traqués par la Gendarmerie. Interviews de cybergendarmes à l'appui. Après deux jours à écouter les professionnels de la cybersécurité, on peut affirmer que leurs préoccupations sont plutôt d'ordre économique et militaire.[18] Et pour cause. Les États-Unis mènent des opérations contre l'Iran. La Chine aurait lancé une offensive contre le *New York Times* en représailles à leurs révélations sur la fortune personnelle du premier ministre chinois. L'entreprise française Bull a vendu son système d'interception de courriers électroniques *Eagle* à Kadhafi. L'agence de renseignement américaine NSA a conclu un accord avec Google pour protéger la firme de cyberattaques. L'été dernier, 30 000 ordinateurs de la compagnie pétrolière d'État saoudienne ont perdu la totalité de leurs données. Le 29 septembre 2011, *L'Expansion* révèle que l'intranet du groupe nucléaire Areva a été visité pendant deux ans depuis des serveurs asiatiques : « *On évoque des préjudices "sur le plan stratégique", ce qui pourrait signifier le vol de secrets industriels. On ignore si les activités militaires d'Areva ont été touchées.* » Malgré Anonymous ou Wikileaks, menaces citoyennes, ces exemples montrent que les nécessités de la cyberdéfense regardent avant tout les industriels se menant une guerre de la connaissance scientifique pour protéger leurs nuisances technologiques, commerciales et militaires. Au temps pour les entreprises et centres de recherche lillois.

Bien sûr, le contrôle électronique concerne aussi la population. Que ce soit pour gérer notre cybervie quotidienne, comme nous l'avons vu plus avant avec la ville intelligente. Ou pour espionner les contestataires et réprimer les auteurs d'événements nuisibles à la marche du commerce et de l'ordre social. Dernièrement, EDF s'est payée le concours d'une entreprise d'« intelligence » économique pour s'introduire dans les ordinateurs de Greenpeace et prévenir leurs activités militantes autour du chantier de l'EPR à Flamanville. Pendant le FIC 2013, la police de Manchester est venue témoigner qu'« *elle ne peut plus se passer des réseaux sociaux.* » Lors des émeutes de l'été 2011, elle a pu collecter des informations en temps réel grâce aux délateurs, « *publier des photos et ainsi identifier les émeutiers. Des messages publiés par la police sur Twitter ont été transférés à des milliers, voire parfois des millions de personnes* », se souvient le *webmaster* de la police de Manchester. La répression est presque omnisciente. Plus de 1 700 personnes arrêtées pour trois jours d'émeutes localisées et quelques vitrines brisées, on mesure l'efficacité des réseaux sociaux, des téléphones portables, des caméras de surveillance, et la réalité du rapport de force actuel entre le pouvoir et ses sujets. Et encore, ils n'avaient pas de carte de vie quotidienne.

L'authentification des utilisateurs de services numériques préoccupent de plus en plus les pouvoirs publics. La lutte contre l'usurpation d'identité devient urgente pour déjouer les arnaques et gagner la confiance des consommateurs dans le e-commerce. D'où l'identification biométrique réputée infalsifiable ; le projet, finalement rejeté par le Conseil constitutionnel, de carte nationale d'identité biométrique équipée d'une seconde puce RFID dédiée au e-commerce ; ou le projet de

18 Préférant quelques criminels en liberté plutôt qu'une population entière sous contrôle, ceci n'est pas un regret mais un constat.

standardisation des signatures électroniques « Idénum » relancé par la ministre Fleur Pellerin pendant le FIC 2013. Pour les pouvoirs publics comme la grande distribution, l'idéal serait un moyen unique d'identification, valable pour tous les services (commerciaux, policiers, sociaux) et toute l'Europe.
Didier Trutt, président de l'Imprimerie nationale, milite pour sa boutique et la mise en fiche de la population : « *Il y a urgence à sécuriser les identités numériques pour se soustraire aux fraudes et protéger sa vie privée. Mais aussi pour alléger le nombre d'identifiants et de mots de passe. Des cartes sont déjà déployées pour les professionnels du transport, de la santé, de la gendarmerie ou de la police. Ce sont des exemples concrets d'identité professionnelle où l'on vient protéger nos accès physiques et informatiques. Ensuite on aimerait bien avoir une identité numérique citoyenne, non falsifiable et régalienne qui soit équivalente et transposable avec l'identité physique, l'état civil. L'Espagne, l'Allemagne ou la Belgique ont décidé de développer une carte nationale d'identité numérique qui sécurise leurs citoyens. D'autres pays utilisent d'autres supports comme une clé USB. Le problème qui est posé est celui de l'enrôlement. Car si cet enrôlement est déficient, vous ouvrez la porte à ce que quelqu'un utilise votre identité. Mais à partir du moment où l'enrôlement est sécurisé, vous avez un point de départ pour une identité numérique. Il faut un référencement national et interopérable pour développer l'économie numérique.* » Anonymat et liberté sont peu de choses face aux nécessités supérieures du commerce en ligne. Le fichage servant autant la croissance que la sécurité.

À tous ceux qui, lors du Forum, ne s'inquiétaient pas de cette identification unique, la députée européenne Marielle Gallo leur a glissé que les députés des anciennes dictatures socialistes étaient réticents à l'idée d'un grand fichier. Allez savoir pourquoi. Quant aux autres qui espéreraient de l'Europe qu'elle vote un « droit à l'oubli » sur Internet – c'est-à-dire la possibilité de « disparaître » de la toile –, elle leur a dit que ce « *droit à l'oubli numérique est une disposition impossible à appliquer sur un plan technologique. [Et qu'il] est malsain de raconter des histoires aux citoyens* » (FIC 2013). Vous ne supprimerez peut-être jamais vos « traces » personnelles laissées sur la toile. Qu'en sera-t-il de vos déplacements, lectures, habitudes d'achat une fois votre « carte de vie quotidienne » vissée dans la poche ?

Avec ces projets de ville intelligente, le filet électronique se resserre contre nous et de manière presque irréversible. Souvenez-vous des malfaiteurs : Raouti Chehi, Chekib Gharbi, Cédric Hozanne, Isam Shahrour, Éric Quiquet, Pierre de Saintignon et les autres.

Solange Ghernaouti, une prof d'informatique spécialiste en cybercriminalité, est venue en rajouter une couche dans la cybervie qui nous menace réellement : « *Cette connectivité permanente et sans contact, c'est l'internet des personnes, or il s'avère que les objets sont connectés de plus en plus à Internet. C'est de la communication entre objets qui va envahir notre espace domestique mais aussi notre espace public comme par exemple les feux de signalisation commandables à distance. Avec la présence des puces RFID et cette prolifération des capteurs qu'on peut intégrer à tous les environnements, on voit apparaître une potentialité de piratage importante et des impacts sur la sécurité des personnes. Et là je n'ai pas encore évoqué l'apparition de ces interfaces neuronales qui permettent de téléguider les ordinateurs par la pensée mais qui, dans le sens inverse, permettraient aussi de pirater les cerveaux. Parallèlement, on a vu apparaître une massification des données par les réseaux sociaux, par cette quantification de soi, par cette mise en scène de soi qui a développé un véritable marché des données à visée marketing, notamment grâce à la géolocalisation et à l'ingénierie sociale. L'humain est à la fois au cœur et perdu dans le cyberespace.* » Non seulement nous sommes de plus en plus aliénés aux ordinateurs, dépossédés d'un environnement qui s'actualise sans nous, mais également en proie à la malveillance des publicitaires, des flics, des urbanistes.

Au delà des aspects strictement sécuritaires, le développement de l'informatique et de « l'intelligence ambiante » est un travail quotidien que mène le pouvoir (élus, industriels, chercheurs) contre notre liberté – celle des sujets, des sans grade. Il crée un monde asymétrique. *Eux* nous gèrent et nous surveillent. Et *nous* sommes gérés et surveillés. Ce n'est jamais l'inverse.
Si l'ordinateur (étymologiquement, mettre de l'ordre) peut marginalement être utilisé pour tenir des blogs contestataires ou éditer des journaux alternatifs, son usage principal et immédiat est celui de guider à distance une usine, un missile, une ville entière. C'est celui de prédire, suggérer, encadrer nos comportements par le calcul statistique, la surveillance et le contrôle.
Ce n'est pas la cybersécurité que nous refusons, mais la cybervie.

C'est pourquoi il faut fermer Euratechnologies.

Hors-sol
Février 2013

Contact : hors-sol[At]herbesfolles.org