Avec

PROSPECTIVE TECHNOLOGIQUE ET PROSPECTIVE TERRITORIALE – HORIZON 2030

FICHE VARIABLE

TECHNOLOGIES DE L'IDENTITE, DE LA SECURITE ET DE LA TRAÇABILITE

Synthèse – avril 2008

Les relations entre réseaux, informatique et sécurité concernent les territoires de trois manières :

- ***La sécurité des systèmes informatiques**, des réseaux et des infrastructures de communication, devient une composante comme les autres de la sécurité publique ;*
- ***L'usage des technologies numériques au service de la sécurité publique et privée** (surveillance, gestion des risques, police…) s'accroît et se sophistique ;*
- ***Le développement rapide et à grande échelle des technologies de sécurité rencontre également des résistances** qui peuvent être juridiques, politiques, ou économiques.*

Pour télécharger la fiche complète :
http://www.la27eregion.fr/Technologies-et-prospective-territoriale

Tableau récapitulatif des impacts sur les territoires, par compétences :

http://www.la27eregion.fr/IMG/pdf/ProspecTIC_impacts_synth.pdf

Ces fiches variables, produites par la Fing et le Lipsor avec le soutien de la Caisse des Dépôts et de la Diact, peuvent être librement téléchargées, utilisées (notamment dans le cadre d'exercices de prospective territoriale) et modifiées, sous réserve d'en indiquer la source : "*Fiche variable de prospective technologique produite par la Fing et le Lipsor avec le soutien de la Caisse des Dépôts et de la Diact*".

EN UNE PAGE...

Parce que l'activité des administrations, des entreprises et des citoyens qui y vivent dépend de manière croissante de l'informatique et des réseaux, les territoires sont directement concernés par les risques informatiques d'une part, et par l'usage à des fins sécuritaires des technologies numériques d'autre part.

Selon la manière dont ces technologies se développent et se mettent en œuvre, les territoires feront en effet face à de nouveaux défis et de nouvelles opportunités :

- **Sécurité des systèmes informatiques et des réseaux :**

▪ De nouveaux risques et de nouvelles formes d'insécurité émergent, face auxquels les collectivités locales (certes moins que l'Etat) seront appelées à réagir.

▪ En tant qu'organisations, les collectivités locales devront assurer leur sécurité informatique et celle de leurs "e-services". En outre, les réseaux constituant désormais une "infrastructure critique" au même titre que les routes, leur éventuelle déstabilisation pourrait être très dommageable pour leur territoire.

- **Usages des outils et réseaux numériques à des fins de sécurité et de traçabilité :**
    - Les acteurs publics disposent de moyens de surveillance de plus en plus puissants de leur territoires (incendies, événements naturels…), de l'activité économique (traçabilité)… et de leurs habitants (santé publique, vidéosurveillance…).
    - Ils devront faire des choix difficiles en face d'exigences contradictoires. Ils auront un rôle de régulation sur certains dispositifs privés, soit pour les rendre moins intrusifs, soit pour s'assurer de leur interopérabilité avec les systèmes publics. Ils pourront être tenus pour responsables de dysfonctionnements, d'insuffisances ou d'abus, des dispositifs de sécurité.
- **Impact sociétal de l'usage sécuritaire des outils numériques :**
    - Le déploiement de dispositifs d'identification et de surveillance, deviendra tôt ou tard un sujet politique important autour de l'arbitrage entre sécurité, vie privée et libertés individuelles.
    - Il aura par ailleurs des conséquences (mal connues aujourd'hui) sur les dynamiques sociales du territoire : évolution ou déplacement de la délinquance, confiance ou défiance entre les citoyens ou vis-à-vis des autorités, accélération ou blocage de l'e-administration ou du vote électronique...

Alors que l'univers numérique s'est longtemps peu préoccupé de sécurité, la montée des risques informatiques d'une part, celles des attentes sécuritaires de la société de l'autre, ont récemment produit un retournement. La sécurité informatique devient une préoccupation majeure, et tous ceux qui jouent un rôle dans les infrastructures et les échanges numériques sont conviés à y contribuer. La vidéosurveillance, le croisement de données publiques, la biométrie, la traçabilité, se développent dans une optique de sécurité publique. Beaucoup de ces dispositifs sont avant tout locaux. Et c'est également au niveau local que des résistances pourraient se développer face à ce qui pourrait ressembler à un contrôle excessif de la société et une agression contre la vie privée.

Les acteurs des territoires auront donc des choix à faire, des investissements à prévoir, des comportements à faire évoluer, des débats publics à organiser. La sécurité informatique et la sécurité "par" l'informatique font désormais partie des tâches des collectivités locales et des questions politiques auxquels ils devront répondre.

DE QUOI S'AGIT-IL ?

Les relations entre réseaux, informatique et sécurité concernent les territoires de trois manières :

- **La sécurité des systèmes informatiques**, des réseaux et des infrastructures de communication, devient une composante comme les autres de la sécurité publique ;
- **L'usage des technologies numériques au service de la sécurité publique et privée** (surveillance, gestion des risques, police…) s'accroît et se sophistique ;
- **Le développement rapide et à grande échelle des technologies de sécurité rencontre également des résistances** qui peuvent être juridiques (protection de la vie privée) politiques (défense des libertés), économiques (arbitrage entre défense de la propriété intellectuelle et liberté d'innover).

Les technologies relatives à la sécurité peuvent être classés en six domaines, en interaction les uns avec les autres :

- L'identification et l'authentification : dire qui l'on est, savoir à qui l'on a affaire ;
- La sécurité des échanges électroniques : confidentialité, intégrité (le contenu de l'échange ne peut pas être modifié à l'insu d'une des parties), valeur probante ;
- La protection des données et des systèmes : éviter l'accès aux machines, aux réseaux, aux applications et aux données de la part de ceux qui n'y ont pas droit ;
- La traçabilité : pouvoir retrouver avec certitude une information, un document, une personne ou un objet, ou encore retracer leur évolution dans le temps et l'espace.
- La surveillance : placer des capteurs physiques (caméras de vidéosurveillance, capteurs d'incendie, sismographes…) ou logiques (enregistrement de communications, suivi d'itinéraires, historiques divers…) à des fins de prévention, de détection et de réponse à des activités délictueuses ou des catastrophes ;
- La résilience : remettre une infrastructure ou un système en état de fonctionner après un dommage ou une attaque.

Historiquement, la sécurité des systèmes informatiques et des réseaux ne faisait pas partie des préoccupations prioritaires des industriels et des opérateurs. D'autant que les Etats se méfiaient (au point de l'interdire, jusqu'en 1996 en France) de l'usage privé de technologies telles que le chiffrement. Mais la dépendance croissante vis-à-vis de l'informatique (pour le commerce et la production, le fonctionnement de l'administration, etc.) s'accompagne d'une montée des risques et des attaques. Par ailleurs, la demande de sécurité monte partout et incite à exploiter à des fins sécuritaires des technologies en voie de maturation rapide : surveillance (vidéo, capteurs divers), identification biométrique, traçabilité, recherches dans de vastes bases de données, etc.

Depuis 1978 et la loi "informatique et libertés", le développement des technologies sécuritaires se déroule cependant dans un débat et un mouvement de balancier permanents entre la recherche d'une efficacité maximale, et la demande de protection de la vie privée et des libertés.

ÉTAT DES LIEUX

Les principales technologies en synthèse

Chiffrement ("cryptage")	Usages : authentification (s'assurer que son interlocuteur est bien qui il prétend être), sécurité des échanges électroniques Le chiffrement consiste au départ à rendre illisible une communication par quiconque ne dispose pas d'un code de déchiffrement. Si le chiffrement est "asymétrique", celui qui chiffre et celui qui déchiffre utilisent chacun un code public (comme un numéro de carte bancaire) et un code privé (comme le code confidentiel de la carte) qui leur sont propres : cette combinaison leur permet également de vérifier qui est leur interlocuteur, et permet de "signer" numériquement des actes avec un niveau de sécurité juridique équivalent (voire supérieur) à celui de la signature manuscrite.
Biométrie	Usages : identification (savoir à qui l'on a affaire) La biométrie consiste à vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres : caractéristiques physiques (empreintes digitales, iris de l'œil, forme du visage ou de la main, voix, voire ADN) ou comportement (démarche, frappe du clavier, dynamique de la signature manuscrite…).
Rfid (Radio-frequency identification)	Usages : identification d'objets, paiement, contrôle d'accès, traçabilité… La radio-identification est une méthode pour lire des données à distance en utilisant des marqueurs appelés « radio-étiquettes » ("RFID tag" en anglais). Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collées ou incorporées dans des produits. Elles comprennent une puce électronique (qui identifie l'objet et stocke parfois quelques autres informations) et une antenne qui lui permet de répondre aux requêtes radio émises depuis un émetteur-récepteur. Les puces Rfid servent par exemple à identifier des cartes de transport (télépéage, pass "Navigo" en Ile de France…), des palettes et conteneurs dans des entrepots, mais aussi les bagages dans un aéroport, les livres dans une bibliothèque, les chats et les chiens domestiques, les arbres de Paris, etc.
Capteurs	Usages : surveillance, traçabilité… Un capteur est un dispositif qui enregistre et transmet des informations sur son environnement. Il peut s'agir de la température, de l'humidité, de la teneur de l'air ou de l'eau en particules dangereuses, du mouvement… mais les caméras de vidéosurveillance, par exemple, sont également des capteurs, certes sophistiqués. Leurs données sont exploitées par des logiciels de télésurveillance, de gestion du trafic, de surveillance environnementale, etc.

Quelques ordres de grandeur

- Près de la moitié des entreprises ont eu connaissance de tentatives d'intrusion dans leurs systèmes et d'autres incidents de sécurité informatique.
- Le Computer Security Institute américain chiffre la même dépense, par employé, à 956 euros / an pour les PME et 200 euros / an pour les plus grandes entreprises.
- Près d'un tiers des ordinateurs au monde ont déjà été infectés par un virus.
- En 2007, 54 millions de cartes bancaires à puce circulent en France, autant de cartes Vitale et plusieurs dizaines de millions d'autres cartes à puce.
- Le déploiement des passeports sécurisés, dotés d'une puce RFID qui contient une photo numérisée et (partir de 2009) les empreintes digitales du titulaire, est engagé. La carte d'identité sécurisée, utilisant les mêmes technologies, est retardée mais pas abandonné.
- Plus d'un milliard d'étiquettes Rfid (identification par radio-fréquences) ont été utilisées en 2006, principalement dans la logistique, le paiement et les transports.
- On estime à plus de 5 millions le nombre de caméras de surveillance dans les espaces publics en Grande-Bretagne, et 25 à 30 millions leur nombre dans le monde.

Les technologies de la sécurité dans les territoires : quelques exemples

- En 2007, un million de français ont, pour la première fois, utilisé des machines pour voter lors d'élection nationales. Mais ces machines se heurtent à de fortes résistances et créent en elles-mêmes une incertitude, du fait des doutes sur leur niveau de sécurité. Plusieurs articles, campagnes d'opinion et pétitions, on demandé un moratoire en attendant, en particulier, l'accès libre au code du logiciel des machines pour en vérifier la robustesse et la transparence.
- En juin 2003, pour accompagner le développement de la vidéosurveillance, la Ville de Lyon s'est dotée d'un "Collège d'Ethique de la Vidéosurveillance des Espaces Publics" et d'une charte d'éthique. La charte renforce notamment l'information du public dans les sites vidéosurveillés et précise les conditions d'accès aux images enregistrées. Elle prévoit que les enregistrements sont détruits au bout de huit jours, au lieu d'un mois comme le stipule la loi. La Ville s'engage également à assurer la formation déontologique des agents d'exploitation du réseau.
- Les 95 000 arbres de Paris sont tous greffés d'une puce RFID. Les bûcherons de la Ville de Paris se déplacent désormais avec une tablette graphique sur laquelle il peut obtenir en direct la fiche de l'arbre ou de l'alignement concerné.
- Grenoble et la société Blue Eye Video ont été nominés aux fameux "Big Brother Awards" de 2005 pour avoir "mis en place un quadrillage vidéo dans le quartier Villeneuve, réputé comme sensible".

ELÉMENTS DE PROSPECTIVE

Si la tendance à un usage de plus en plus sécuritaire de l'informatique et des réseaux ne fait pas de doute (le développement de la vidéosurveillance faisant par exemple partie des tendances certaines), la tension entre sécurité, contre-attaques techniques, inertie des comportements et enfin, résistance citoyenne ou institutionnelle, peut aboutir à plusieurs points d'équilibre très différents.

L'hypothèse tendancielle : 2030, tension durable

La généralisation et l'omniprésence du numérique et des réseaux produisent à la fois de nouveaux risques, de nouvelles réponses à ces risques, de nouveaux usages sécuritaires des technologies et des résistances vives, sans aboutir à un point d'équilibre stable. Des attaques informatiques coordonnées contre une entreprise ou un territoire font régulièrement partie de l'actualité. L'abondance des traces, des dispositifs de surveillance et des modes de collecte d'informations ont rendu inopérantes les protections traditionnelles de la vie privée, mais d'autres dispositifs savent tromper les systèmes de surveillance, effacer les données ou les recouvrir d'informations inexploitables, etc. De nombreux groupes et associations s'opposent, parfois violemment, à la "surveillance généralisée". Les technologies de surveillance contribuent à la sécurité publique, mais la criminalité organisée sait mieux y échapper que les petits délinquants.

Les territoires sont au cœur de cette tension. D'un côté, on attend de ceux qui les gèrent d'être capable de de prévenir les risques et la délinquance plutôt que d'y répondre. De l'autre, on leur reproche de tout savoir et tout contrôler. Et par surcroît, ils sont structurellement démunis devant la sophistication croissante des moyens techniques dont disposent les groupes organisés et déterminés à contourner leurs dispositifs sécuritaires.

Trois variantes possibles

Le déploiement des technologies sécuritaires peut prendre des directions très différentes en fonction de deux facteurs : l'arbitrage collectif entre sécurité d'une part, de libertés individuelles et publiques de l'autre ; et la capacité (ou non) des techniques et des politiques de sécurité de produire des réponses réellement cohérentes, efficaces et durables aux menaces.

- **Hypothèse 1 – Le choix des libertés**

  La multiplication des puces suscite des inquiétudes, voire de véritables rejets. Vers 2012-2015, la plupart des sociétés européennes choisissent de préférer un certain niveau de risque aux contraintes imposées par la recherche d'une sécurité quasi-absolue. réglementés. Les moyens se déplacent depuis la prévention vers la réponse rapide aux événements ; des évolutions juridiques réduisent l'exposition des décideurs aux conséquences d'événements imprévisibles. Les restrictions imposées au croisement de fichiers rendent plus difficile le développement de services avancés d'e-administration. Les gains de productivité dans les administrations publiques sont réduits, ce qui favorise le développement d'alternatives privées.

- **Hypothèse 2 – Le choix de la protection**

  La persistance du sentiment d'insécurité ouvre la voie à la surveillance généralisée et appuyée sur des dispositifs techniques. La sécurité s'impose comme la priorité dans le développement et le déploiement des technologies de l'information – y compris au détriment d'une part de rêve et d'innovation. On attend des entreprises, des territoires et des institutions qu'ils préviennent les événements désagréables (accidents, délinquance, catastrophes…), plutôt qu'ils ne les réparent.

  Les territoires sont chargés d'installer et d'interconnecter les dispositifs de surveillance et de traçabilité et de contribuer à la sécurisation des réseaux présents

sur le territoire. Disposant d'informations sans cesse plus riches et complètes, leurs responsabilités en matière de prévention des risques s'étend sans cesse.

- **Hypothèse 3 – Le choix de la transparence**

  Entre demande de sécurité et inquiétudes pour les libertés, l'équilibre paraît impossible à trouver et aboutit à un constant mouvement de balancier. En définitive, chacun finit par organiser pour lui-même sa sécurité et la protection de son périmètre privé. Tout le monde est à la fois surveillant et surveillé, tout le monde s'efforce de défendre sa vie privée tout en s'intéressant à celle des autres. Les entreprises et les acteurs publics sont eux-mêmes surveillés et sommés de devenir transparents. Organisés en communautés, les citoyens réfléchissent ensemble à leur sécurité, voire, prennent en charge certaines tâches en matière de sécurité et d'ordre public, à la place des acteurs publics.