Note numéro 8
décembre 2014

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Villes intelligentes et Normes de qualité : Impacts sur les politiques publiques de sécurité

Les espaces urbains concentrent 53% de la population mondiale. Ce chiffre devrait atteindre le seuil de 70% d'ici 2050. Pour mémoire, l'INSEE[1] définit la ville comme tout espace présentant une certaine continuité d'habitat, constituée soit d'une commune composée de plus de 2000 habitants, soit de deux ou plusieurs communes sur le territoire desquelles une zone agglomérée comprend plus de 2000 habitants. Les décideurs publics sont confrontés à des défis majeurs : la mobilité urbaine, la demande énergétique et la garantie de la sécurité des habitants. Tout naturellement, le développement de la ville intelligente va modifier de manière substantielle les politiques publiques de sécurité s'agissant aussi bien des systèmes d'information que du contrôle des flux. Parallèlement, ce développement va s'accompagner de la création d'indicateurs pertinents qui seront censés mesurer les points de performance. Précurseur en la matière, la norme ISO 37120 : 2014 relative au « *Développement durable des collectivités -- Indicateurs pour les services urbains et la qualité de vie* » recense pour la première fois, dans un document officiel, les items qui serviront à mesurer les performances dans les domaines fondamentaux.

Les espaces habités auront recours aux architectures intelligentes. Déclinées sur le plan sécuritaire, les architectures intelligentes disposeront de capteurs implantés dans les vecteurs de communication, les lieux publics et les locaux à usage d'habitation ou professionnel. Ces architectures numériques procéderont au recueil d'une multitude de données à forte valeur ajoutée pour les décisions de mise en œuvre des politiques publiques de sécurité. L'exercice des missions traditionnelles de la gendarmerie va connaître des changements majeurs.

La quantité de données recueillie pose nécessairement la question de la préservation des libertés individuelles, dont le respect de la vie privée est une des composantes majeures. En retour, elle ouvre aussi de formidables opportunités de constatation, de recueil d'indices utiles à la résolution de certains crimes et délits. À ce propos l'avis de la CNIL sur les compteurs communicants dans le pilotage énergétique du logement mérite une attention toute particulière. À ce stade, la sécurité de l'internet des objets connectés a de plus en plus à prendre en compte la possibilité qu'un tiers prenne le contrôle du système de commande d'une application d'architecture intelligente.

La ville intelligente et ses applications dérivées ouvrent un vaste chantier de réflexion et de doctrines pour les années à venir en matière de politique publique de sécurité et de modes d'action dans les missions clés de police administrative et de police judiciaire.

La norme ISO 37120 : Développement durable des collectivités -- Indicateurs pour les services urbains et la qualité de vie : Enjeux et perspectives

Une norme est un document contenant des exigences articulées plusieurs volets. Nous assistons à une révision des normes ISO afin de les adapter aux changements du monde et aux attentes des différentes parties. Première dans le genre, la norme ISO 37120, publiée le 14 mai 2014, se propose de répondre aux attentes fortes en matière de recensement et analyse des indicateurs existants sur le développement durable et la résilience des villes. Véritable outil de la performance, la norme 37120 pourrait être l'outil d'évaluation de la qualité des villes et de leur niveau d'avancement par les 17 domaines abordés et les avantages escomptés.

Déclinée localement, cette norme constituera un outil de pilotage et de contrôle de gestion des

1 http://www.insee.fr/fr/methodes/default.asp?page=definitions/ville.htm

différentes politiques publiques. Il convient de souligner que cette norme est à destination de toute ville, municipalité ou collectivité désireuse d'évaluer sa performance de façon comparable et vérifiable, quels que soient sa taille, sa situation géographique et son niveau de développement.. À l'évidence cette norme aura vocation à s'appliquer sur les zones rurales et péri-urbaines ainsi que les voies de communication. Document élaboré par l'Organisation Internationale de Normalisation (OIT), il a vocation à être révisé, amendé ou complété dans le temps. L'agence française de normalisation (l'AFNOR), chargée de la transcription de ce document, prévoit la publication de la version nationale en avril 2016. Sur les 17 indicateurs principaux retenus, le volet Sécurité repose sur 5 indicateurs de base ou de soutien considérés comme efficients dans ce segment : nombre d'agents pour 100 000 habitants (indicateur de base) , nombre d'homicides pour 100 000 habitants (indicateur de base), atteintes aux biens pour 100 000 habitants (indicateur à l'appui), délai de réponse pour le département de police depuis l'appel initial (indicateur à l'appui), taux d'atteintes aux personnes pour 100 000 habitants (indicateur à l'appui).

Pour lutter efficacement contre les atteintes aux personnes et aux biens, améliorer les délais de réaction entre la survenance d'un événement et la réponse à apporter, les architectures intelligentes apporteront une contribution décisive dans l'efficience des politiques publiques de sécurité.

Les architectures intelligentes, auxiliaires de la sécurité des personnes et des biens

Il n'existe aucune définition officielle de l'architecture intelligente. La doctrine[2] a pu définir l'architecture intelligente comme l'ensemble des éléments spatiaux et architecturaux ayant la capacité de répondre intelligemment à l'environnement extérieur ainsi qu'aux besoins des usagers. Ces architectures intelligentes reposent sur un réseau de capteurs sans fil qui récupèrent les données, pierre angulaire de l'architecture intelligente.

Parmi les architectures intelligentes, certaines ont une vocation sécuritaire dès leur conception comme les systèmes de vidéo-protection et la biométrie. La vidéo-protection connaît une évolution de plus en plus sophistiquée qui dépasse largement la fonction initiale de surveillance qui lui était assigné à l'origine. Ainsi, dans un espace donné, doté de contrôles d'accès et de caméras, un centre d'hypervision peut réaliser une prestation de type escorte d'accompagnement pour permettre à une personne de se déplacer en toute quiétude d'un point à l'autre de cet espace connecté.

La sécurisation des espaces à vocation communautaire comportera progressivement un système de dispositif global de sûreté qui intégrera l'ensemble des sous-systèmes : vidéo-surveillance, contrôle d'accès, système anti-intrusion et interphonie dans l'espace public. Le château de Versailles[3] est un exemple type de ce que la technologie actuelle est capable de faire en termes de centre d'hypervision. Ce concept serait, sous réserve d'adaptation, transposable quelles que soient la taille et la nature de l'espace à connecter.

La biométrie[4] est le deuxième « silo » intelligent au service de la sécurité. La CNIL définit la biométrie comme « l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses

2 Khaled Sherbini, Robert Krawczyk, Overview of intelligent architecture : 1st ASCAAD International Conference, e-design in Architecture KFUPM, Dhahran, Saudi Arabia, 12-2004

3 http://www.assystem.com/fr/entreprise/livre-blanc-introduction.html

4 http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/biometrie-des-dispositifs-sensibles-soumis-a-autorisation-de-la-cnil/

caractéristiques physiques, biologiques, voire comportementales ». Les données biométriques sont classées en trois catégories qui répondent aux critères suivants : les prélèvements du corps humain (l'ADN, l'odeur corporelle) ; les représentations numériques ou gabarit (l'empreinte digitale ou le contour de la main) ; les attitudes ou comportements (signature manuscrite, frappe sur un clavier)

Les applications opérationnelles en terme de sécurité sont sans limite, notamment la biométrie comportementale. Le Groupe de l'article 29[5] précise que « les techniques biométriques basées sur le comportement visent à mesurer les caractéristiques comportementales d'une personne. Elles comprennent la vérification de la signature manuscrite, l'analyse de la frappe sur le clavier, l'analyse de la démarche, la manière de marcher ou de se mouvoir, des modèles indiquant une certaine pensée subconsciente comme le mensonge, etc... »

Le mobilier urbain offre des opportunités au service des architectures intelligentes. Il en est ainsi des candélabres installés sur la voie publique. Ces objets deviennent de précieux auxiliaires de la sécurité et de l'ordre publics. Maillant depuis plus d'un siècle l'espace public de la métropole jusqu'au hameau, les candélabres constituent, par leur structure et leur implantation, le support idéal de l'infrastructure numérique sans fil qui contrôle, surveille et maintient le monde sensoriel par les données valorisables recueillies par ces capteurs[6]. Une liste non-exhaustive permet d'en mesurer rapidement l'intérêt : diffusion d'annonces et d'alertes, captation d'image, comptage de passants, détections de mouvements de foules anormaux, voire spontanés. Ce même éclairage public pourrait être en mesure de fonctionner selon la fréquentation d'une rue et de fournir des informations concernant le nombre d'individus.

Ces quelques cas concrets soulèvent de nouvelles problématiques en terme d'intégrité des systèmes de commande. Le contrôle du système par son légitime utilisateur demeurera le facteur clé de toute réussite dans le déploiement d'architectures intelligentes des espaces connectés. Pénétrer un système informatique qui pilote des fonctions critiques peut avoir des conséquences graves. Le vol par un cambrioleur agissant par effraction « numérique » ne sera pas une vue de l'esprit. L'hypothèse d'un mode opératoire consistant à détourner les systèmes Smart pour savoir si une personne est présente à son domicile et ainsi désactiver les mécanismes de sécurité sera très plausible. Cette mutation exigera que les locaux à usage d'habitation ou professionnel soient inviolables et que les systèmes embarqués le soient tout autant.

Les données personnelles ou publiques, collectées dans le cadre des architectures intelligentes, présentent un caractère valorisable qu'il convient d'encadrer. Sur cette problématique, la CNIL se positionne dès à présent comme l'autorité de régulation incontournable dans la surveillance numérique.

Des évolutions suivies de près par la Commission nationale informatique et liberté (CNIL)

En France, la CNIL a commencé à se saisir des problématiques des données collectés sur des objets connectés dans le secteur des réseaux de distribution d'électricité intelligents (les « smarts grids »[7]). Elles préfigurent les obligations des opérateurs vis-à-vis des clients en leur qualité de citoyen.

La CNIL pose un constat : le caractère « intelligent » attendu des projets de ville numérique provient des données captées par les objets connectés : ce

5 G29 : groupe des autorités européennes de protection des données personnelles

6 Pour des applications concrètes : http://intellistreets.com/index.php

7 http://www.cnil.fr/linstitution/actualite/article/article/compteurs-communicants-premieres-recommandations-de-la-cnil/

ne sont pas les villes qui deviennent intelligentes, mais ce sont leurs données. Ces données, souvent présentées comme anonymes, ne le sont pas toujours, d'autant plus que les techniques de ré-identification de données évoluent sans cesse. Par exemple, un capteur de présence qui pilote l'éclairage public d'une rue peu passante peut permettre de deviner quel riverain est passé, si la temporisation d'extinction des lampadaires est toujours la même.

Ces compteurs communicants suscitent des questions nouvelles en matière de vie privée. Une analyse approfondie des courbes de charge[8] pourrait permettre de déduire un grand nombre d'informations sur les habitudes de vie des occupants d'une habitation : heures de lever et de coucher, heures ou périodes d'absence, présence d'invités dans un logement, prises de douche, nombre de personnes présentes dans le logement, etc. De manière plus globale, la gestion des données, collectées dans le logement et transmises à l'extérieur pour permettre un pilotage à distance de certains équipements domestiques, va élargir le champ des investigations à venir dans le domaine de la police judiciaire. Les locaux à usage professionnel seront interconnectés avec leur environnement média et le reste de la sphère publique. Ces ensembles de « béton intelligent », par leur capacité à réagir aux besoins de leur environnement, garantissent une traçabilité des opérations accomplies. Ils sont aussi en mesure de faire face à toute tentative d'atteinte à leur intégrité comme des actes de malveillance physique ou des cyberattaques. L'efficience de la sûreté et de la sécurité apportées par ces nouvelles technologies devra néanmoins prendre en compte les principes fondamentaux du droit des personnes reconnus dans les sociétés démocratiques, tant dans leur sphère intime que professionnelle.

Ces masses de données à caractère personnel ou public soulèvent d'ores et déjà une nouvelle réflexion sur la recevabilité de la preuve fondée en droit français sur le principe de loyauté et dans son prolongement, le principe d'égalité des armes, principe que la Cour européenne des droits de l'Homme applique avec vigilance. Les nouveaux modes d'investigation ouvrent des perspectives dans la manifestation de la vérité des enquêtes criminelles et délictuelles.

Les process pour assurer la sécurité des personnes et des biens vont se trouver profondément changés par l'implantation de capteurs de données dans les espaces publics comme privés. La connaissance et l'accès des données recueillies devraient, dans la limite des libertés fondamentales et sous le contrôle du juge, être prises en compte dans l'analyse et la lutte contre les phénomènes de délinquance d'une circonscription. Les normes de résilience des espaces connectés et l'efficience dans l'analyse des mégadonnées (Big data) dessinent pour le futur les outils d'aide à la décision des politiques publiques de sécurité.

8 http://www.cnil.fr/documentation/deliberations/deliberation/accessible/non/delib/279/

Mes remerciements vont à Maître Alain Bensoussan, avocat spécialisé dans le Droit des technologies avancées qui a bien voulu m'apporter son expertise dans la rédaction de cette note.
http://www.alain-bensoussan.com/