Conférence Cyber des Collectivités intelligentes (C3I)

Première édition

6 mars 2018 – Paris

COMPTE RENDU

OPENING SESSION

- **Jean-Martin JASPERS**, *Directeur du Centre des Hautes Etudes du ministère de l'Intérieur (CHEMI) et Délégué à la Prospective et à la Stratégie (DPS) du ministère de l'Intérieur*
- **Thierry VINCON**, *Conseiller à Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) du ministère de l'Intérieur*

« ***2016 est l'année de virage ou les vols en cybercriminalité dépassent les vols de voitures et les vols à la tire*** ».
Jean-Martin JASPERS, *Directeur du Centre des Hautes Etudes du Ministère de l'Intérieur et Délégué à la Prospective et la Stratégie (DPS) du ministère de l'Intérieur*

Inhérentes à l'espace numérique, les cyberattaques sont un phénomène relativement récent, mais en pleine expansion : on en compte déjà au moins 450 000 annuelles à l'encontre de PME-PMI en France. Néanmoins, les collectivités territoriales échappent à cette menace. Le ministère de l'Intérieur fait le constat que la France reste relativement bien préservée du cyber-risque grâce à de bonnes politiques publiques en matière de cybersécurité.

Par exemple les ransomwares qui sont un phénomène d'attaque en plein développement, touchent aujourd'hui peu les collectivités, même si cela risque de changer. La raison majeure d'une telle « désaffection » des attaquants réside dans le fait que pour une entreprise une rupture de l'activité due à une paralysie de ses systèmes d'information constitue une perte directe de revenus : celle-ci sera donc plus à même de payer une rançon en cas de rançongiciel qu'une collectivité territoriale. Néanmoins, ce type d'attaques risque de concerner de plus en plus les collectivités étant donné les données qu'elles possèdent.
La protection de la data représente donc une question majeure dans les process de collectivités intelligentes.

Face à ce phénomène, le ministère de l'Intérieur a engagé une réflexion pour accompagner les collectivités quelle que soit leur taille, dans ces process de smart city et de territoires intelligents. Une des questions qui en ressort est de savoir à quel niveau doit être élaborée la politique de cybersécurité du ministère à destination des territoires et des collectivités territoriales. Le niveau départemental semblerait à ce titre le plus à même de répondre aux différents enjeux, notamment la définition et la mise en place d'une gouvernance efficace, alliée à des réseaux de ressources et de compétences mutualisés.

« ***L'enjeu n'est pas de parvenir à freiner ce qui est en train de se passer, mais c'est de réussir à adapter l'ensemble des organisations aux changements*** ».
Thierry VINCON, *Conseiller à Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) du ministère de l'Intérieur*

Par ailleurs, la France dispose des atouts nécessaires pour devenir une puissance mondiale en matière de cybersécurité : 5e puissance économique mondiale, elle doit aujourd'hui travailler à l'être aussi en matière de sécurité numérique. Plusieurs pistes d'action semblent se dégager : affirmation d'un véritable leadership dans la gestion des données publiques de la part de l'Etat central, inclusion pleine et entière des citoyens dans le processus de cybersécurité, ainsi que sensibilisation de tous aux différentes règles d'hygiène de sécurité numérique, indispensable pour instaurer une culture commune de cybersécurité.

PREMIERE TABLE RONDE

LE CHAMP DES ENJEUX DE SECURITE NUMERIQUE POUR LES COLLECTIVITES TERRITORIALES

- Animateur : **Bénédicte PILLIET,** *Directrice du CyberCercle*
- **Luc BELOT**, *ancien Député de Maine-et-Loire (XIVème Législature) et auteur du rapport d'information au Premier Ministre "De la smart city au territoire d'intelligence(s) – l'avenir de la smart city"*
- **Bruno HERVET**, *Vice-président exécutif Smart & Resourceful Cities de Suez*
- **Denis HAMEAU**, *Conseiller communautaire de la Métropole de Dijon*
- **Jean-Martin JASPERS**, *Directeur du CHEMI et DPS du ministère de l'Intérieur*

Avant toute chose, il est indispensable de prendre conscience que la cybersécurité n'est pas uniquement un sujet relevant des directions de sécurité informatique (DSI), mais qu'il s'agit d'un sujet plus large relevant du développement et de l'attractivité des territoires. Une stratégie de cybersécurité efficace doit consister en une dynamique impliquant l'ensemble de l'écosystème local, peut-être avec un pouvoir départemental renforcé, et sortir des cloisonnements techniques dans lesquels elle est trop souvent enfermée pour créer une culture cybersécurité commune dans l'ensemble des directions.

La formation de l'ensemble des fonctionnaires et agents de la fonction publique doit en ce sens être une priorité. Ainsi la campagne de phishing menée fin 2017 par le Directeur de la sécurité informatique de Bercy à destination des 130 000 fonctionnaires du service est un exercice qui se doit d'être généralisé tant les résultats ont été révélateurs : en deux heures, 30 000 clics sur l'email frauduleux ont été réalisés, venant de tous les niveaux hiérarchiques…

Sur les 25 recommandations du rapport d'information « De la Smart City aux territoires intelligents – l'avenir de la Smart City » remis par Luc BELOT au Premier ministre en 2017, quatre avaient trait à la cybersécurité, dont deux à la formation : formation des cadres territoriaux et formation des élus. Dans l'ensemble des projets numériques à l'heure actuelle, aucun ou très peu intègrent l'une de ces quatre recommandations en matière de cybersécurité. Le maillon faible de la cybersécurité, c'est le facteur humain : la sensibilisation et la formation des agents mais aussi plus largement de l'ensemble de la population sont donc les deux piliers de la sécurité numérique.

> « ***La Smart City représenterait à l'horizon 2020 un marché de plus de 1 400 milliards de dollars, dont seulement 77 millions de dollars prévus pour répondre aux enjeux de sécurité numérique... Ce n'est pas assez !*** »
> **Luc BELOT**, *ancien député de Maine-et-Loire (XIVe Législature), auteur du rapport d'information « De la Smart City aux territoires intelligence(s) – l'avenir de la Smart City »*

L'Estonie est considérée par le ministère de l'Intérieur et plus particulièrement le CHEMI, comme un modèle de référence en ce qui concerne la protection des données personnelles, ayant adopté des règles relativement fermes en

la matière. Si un agent public accède aux données d'un citoyen, celui-ci reçoit un mail l'avertissant de ladite consultation, et est en droit de demander la preuve de l'autorisation administrative d'une telle consultation de la part du fonctionnaire. Si celui-ci ne peut fournir cette autorisation, son renvoi est immédiat. De telles règles ont permis de créer un véritable cadre de confiance pour les citoyens, qui doit être à la base de tout projet numérique. Dans le cadre des projets de collectivités intelligentes, il est indispensable de garantir aux citoyens et aux usagers que leurs données sont sécurisées. C'est en ce sens que le RGPD est une brique intéressante.

Malheureusement, très peu de structures seront prêtes pour le 25 mai 2018, date limite de mise en conformité pour le RGPD : moins de 10% des entreprises ou des collectivités territoriales seront en conformité. Par ailleurs, le nouveau poste créé par le RGPD, le Délégué à la Protection des Données personnelles (DPO pour Data Privacy Officer), aura besoin de ressources attribuées et d'une formation solide. Or certaines collectivités territoriales n'ont pas même les moyens d'embaucher un technicien informatique : même si elles ont la volonté de se mettre en conformité avec le RGPD, elles ne disposent pas aujourd'hui des ressources humaines et financières pour mener à bien cette dynamique. D'où la nécessité de créer des postes de DPO mutualisés ou au niveau de l'intercommunalité.

Dijon est un modèle de ville intelligente de deuxième génération. La Métropole s'est lancée dans un modèle de management du risque, permettant une révolution dans la manière d'envisager la ville et la Métropole intelligentes. Ce modèle se fonde sur : un leadership public de la data ; l'intégration du processus de smart city dans une logique de développement durable, de transition écologique et de maintenance urbaine ; l'inclusion des citoyens dans les projets, en les considérants comme « co-constructeurs » du service public, de son amélioration et de l'invention des nouveaux services. L'ensemble du territoire est ainsi intégré dans un projet commun et construit le modèle de la Métropole intelligente. L'objectif est de fournir un modèle de collectivité intelligente offrant une logique d'ensemble, intégrant de la sécurité à tous les échelons du projet, des schémas de résilience et protégeant la data captée dans tous les domaines (la Métropole intelligente étant propriétaire, garante absolue et responsable de leur utilisation, elle doit donc rester maître des données collectées). Sécurisée, cette data devient un levier de développement du territoire grâce au modèle de Smart Métropole, enclenchant une dynamique vertueuse (installation d'écoles d'ingénieurs, développement de projets autour de l'Open Data, des FabLabs, de l'open innovation…). Les conditions de captation, traitement, stockage et autorisations d'accès aux données personnelles et non personnelles sont strictement stipulées dans les contrats qui lient la Métropole aux prestataires de service.

> « ***Une vision stratégique, une connaissance des forces et des faiblesses de son territoire, des projets clairs, des moteurs reconnus, voilà la première étape vers une ville intelligente. Construire celle-ci, c'est avant tout construire la ville inclusive, en rétablissant du lien avec les territoires les plus modestes et incluant dans les projets les citoyens qui se sentent laissés pour compte, dans une véritable logique de territoire*** ».
> **Denis HAMEAU**, *Conseiller communautaire de la Métropole de Dijon*

DEUXIEME TABLE RONDE

S'ORGANISER POUR LUTTER EFFICACEMENT CONTRE LES CYBERMENACES SUR LES SMART CITIES

- Animateur : **Ariel GOMEZ**, *Rédacteur en chef de Smart City Mag*
- **Philippe AGARD**, *Directeur du segment Public Safety & Defense de Nokia*
- **Christophe AUBERGER**, *Directeur Technique de Fortinet*
- **Anne LE HENANFF**, *adjointe au maire de Vannes en charge de la communication, des systèmes d'information et du développement numérique*
- **Jérôme POGGI**, *Responsable de la Sécurité des Systèmes Industriels (RSSI) de la Ville de Marseille et membre de l'Association des Villes et Collectivités pour les Communications électroniques et l'Audiovisuel (AVICCA)*
- **ROGER REY**, *Vice-président du SIDEC du Jura, maire de Conliège et représentant de la Fédération nationale des collectivités concédantes et régies (FNCCR)*

Pour penser et instaurer une véritable collectivité intelligente, tout projet doit s'appuyer sur les infrastructures préexistantes, et intégrer un volet cybersécurité à tous les échelons du projet : il ne suffit pas de proposer une application aux citoyens pour avoir le statut de « smart city » ou de territoire intelligent. Un projet de territoire intelligent doit de plus s'appuyer sur les données comme d'un levier de développement du territoire, données qui doivent être protégées et sécurisées « *by design* » et « *by default* ». La cybersécurité dans ce cadre s'applique notamment à l'ensemble des systèmes qui collectent, stockent, analysent ces données, pour garantir leur protection.

« ***La majorité des codes malveillants est redéveloppée constamment. Pour s'en prémunir, on peut utiliser l'analyse comportementale et l'automatisation afin de détecter les menaces et réagir automatiquement. On réduit ainsi la fenêtre de vulnérabilités*** ».
Christophe AUBERGER, *Directeur Technique, Fortinet*

Seulement 3% des victimes de cyberattaques déclarées aujourd'hui sont des collectivités territoriales. Il n'y a pas de raison de considérer que les collectivités territoriales soient moins des cibles ou des victimes potentielles d'incidents de cybersécurité. Dans le cadre d'une collectivité intelligente, la systématisation de la détection et de la cybersécurité doit devancer la réaction humaine. L'utilisation des réseaux neuronaux et du Deep Learning pour extraire des comportements à risques des téraoctets de données récoltées est une solution avancée par de nombreux experts pour parvenir à un meilleur traitement des incidents de cybersécurité. Changer l'approche et le traitement des cybermenaces est primordial pour l'instauration de la smart city (la durée de vie moyenne d'un code malveillant est estimée aujourd'hui à moins de 24h). L'analyse comportementale peut aussi être l'une des solutions à étudier : 80 % des botnets aujourd'hui ne sont pas détectés sur la signature du code malveillant lui-même, et bénéficient d'une fenêtre moyenne de trois heures avant d'être répertoriés dans une base de données comme code malveillant par un antivirus. L'analyse comportementale peut permettre de combler en partie ce délai. Les solutions proposées ne doivent pas être trop compliquées pour les différentes équipes, solutions qui devront s'accompagner de l'élaboration et la mise en œuvre de politiques de sensibilisation et de formation.

Face à ces bouleversements et ces besoins de changements, les moyens humains et financiers ne suivent pas les besoins en matière de cybersécurité, correspondant à l'un des freins auquel l'ensemble des acteurs fait face aujourd'hui, plus particulièrement les collectivités territoriales. Les ressources humaines sont rares, chères, énormément sollicitées et une collectivité ne peut pas concurrencer les moyens financiers de grands groupes du privé, parfois étrangers, qui peuvent se permettre des offres alléchantes en matière de rémunération et de cadre de travail.

Les évolutions récentes de la réglementation européenne relative à la cybersécurité vont induire de nouvelles pratiques et de nouvelles approches, qui permettront de sortir de ce paradigme. La véritable révolution copernicienne introduite par le Règlement Général relatif à la Protection des Données (RGPD) qui sera opposable le 25 mai 2018 va forcer un changement de comportement en ce qui concerne le traitement des données à caractère personnel, forçant à la mutualisation des ressources pour les structures modestes, notamment pour les collectivités territoriales. La nomination de Délégués à la protection des données (DPD, ou *DPO – Data Privacy Officer*), la mutualisation de ce dernier pour certaines structures de taille et de moyens modestes, la tenue continue d'un registre, la co-responsabilité pénale liant dorénavant le sous-traitant et le responsable du traitement, sont autant de nouveautés qui vont permettre l'institution d'une plus grande culture de cybersécurité, une révolution des process et des habitudes, et permettront d'établir un cadre de confiance permettant le développement de projets de smart cities plus sûres, bénéficiant de la confiance des citoyens quant au traitement réservé à leurs données personnelles. La smart city cybersécurisée adviendra à travers la mise en œuvre d'une politique globale de cybersécurité.

« ***Lorsque la mairie de Vannes a été attaquée, on a vu notre erreur : faire de la sécurité numérique un sujet technique. Depuis, on a monté la responsabilité d'un cran, convaincu le maire et la Direction générale des services, mis en place une politique dédiée, impliqué l'ensemble des services, débloqué un budget. La mise en place d'une politique de cybersécurité conforme au RGPD s'est faite au prix de l'abandon d'autres projets*** ».

Anne LE HENANFF, *adjointe au maire de Vannes, en charge de la communication, des systèmes d'information et du développement numérique*

CLOSING SESSION

- **S.E. Alar STREIMAN**, *Ambassadeur Extraordinaire et Plénipotentiaire d'Estonie en France*

Les principes élémentaires du numérique en Estonie, combinés à la création d'une identité numérique, sont les deux piliers de la politique de cybersécurité développée par le pays.

L'objectif avoué de l'Estonie est de parvenir à un système ne comportant aucune bureaucratie et l'instauration d'une gouvernance numérique internationale. L'espace numérique s'affranchit des frontières nationales, les enjeux de cybersécurité dépassent ainsi les frontières et concernent souvent un grand nombre de pays. La priorité est donc de travailler de concert au niveau des Etats, pour avancer ensemble vers une plus grande cybersécurité. Celle-ci n'est pas un sujet réservé aux techniciens et ingénieurs informatiques, mais relève d'un véritable projet stratégique, qui doit être porté à tous les niveaux de la pyramide politique, économique et sociale, au niveau national et international.

Les citoyens estoniens ont confiance car le système est pratique, rapide et sécurisé. L'utilisation de la technologie Blockchain pour sécuriser ses données nationales permet à l'Estonie de découvrir en temps réel les atteintes ou les tentatives de piratage et de garantir l'intégrité des données à caractère personnel de ses citoyens. L'Estonie veut tendre la main aux autres Etats membres de l'Union Européenne pour travailler de concert et avancer de manière conjointe vers une plus grande sécurité numérique.

L'Estonie se veut un modèle en Europe en matière de numérique : la 4G couvre l'intégralité du territoire ; chaque résident estonien possède une identité électronique, matérialisé sous la forme d'un nombre complexe, attribué à la naissance, qui est la condition permettant un service public numérisé de confiance ; 99% des services publics estoniens sont accessibles en ligne ; 350 millions de signatures électroniques sont utilisées annuellement en Estonie ; 30% des électeurs votent en ligne ; presque 100% des transactions bancaires sont réalisées en ligne…

> « ***Les données personnelles des citoyens ne sont collectées qu'une seule fois, ce qui permet de réduire la bureaucratie et de limiter le risque pour les données personnelles. C'est très important*** ».
> **S.E. Alar STREIMAN**, *Ambassadeur Extraordinaire et Plénipotentiaire d'Estonie en France*