Convergences du droit et du numérique –3ème édition

Contribution à l'atelier

Les responsabilités des collectivités en matière de cybersécurité

Camille Dubedout, doctorante en Droit à l'Université Grenoble Alpes (CESICE) et à l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Communauté d'appartenance : juridique

Problématique visée : Cette contribution propose de s'interroger sur la portée des obligations juridiques qui incombent aux collectivités territoriales en matière de cybersécurité au regard de la numérisation croissante des services publics et de la multiplication concomitante des cyberattaques.

Eléments de la contribution :

Depuis la fin des années 2000, les villes et territoires régionaux voient émerger en leur sein un nombre pléthorique de nouveaux services basés sur la connectivité des réseaux et l'exploitation des flux de données, en particulier via les objets connectés[1]. Un enjeu s'avère cependant sous-estimé par de nombreux acteurs à l'heure actuelle et notamment par les collectivités françaises : la sécurisation des infrastructures, des réseaux et des données. Les dispositifs numériques mis en place dans les villes tels que les caméras, les capteurs et les réseaux se révèlent en effet extrêmement vulnérables à des attaques numériques malveillantes. Des attaquants informatiques peuvent par exemple aisément capter les données sensibles des passants en interceptant leurs connexions sur le wifi public[2]. Ils peuvent également paralyser l'ensemble des services délivrés par la municipalité grâce à une attaque en déni de service, dite « DDos », tel que cela s'est produit en mai 2019 à Baltimore[3]. Plus encore, les infrastructures critiques à l'instar des réseaux d'eau, d'énergies et de circulation routière se révèlent de plus en plus exposées à des attaques informatiques[4].

---

[1] L'Union internationale des télécommunications définit cette technologie1 comme « *l'infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* ». Union internationale des télécommunications (UIT), « Présentation générale de l'internet des objets », Recommandation Y.2060, juin 2012.

[2] Actu Occitanie, « Un hacker pirate le Wi-Fi public, et pénètre les appareils qui y sont connectés », 4 avril 2018.

[3] Le Monde, « Baltimore paralysée par un virus informatique en partie créé par la NSA », 29 mai 2019.

[4] En 2014, une équipe de recherche de l'Université du Michigan a ainsi démontré la facilité avec laquelle il était possible de pirater les feux tricolores de la ville, de modifier leur cadence et de provoquer de fait d'immenses embouteillages voire des accidents en cascade. Voir : Atlantico, « Prendre le contrôle des feux de signalisation en ville : un jeu d'enfant pour les hackers », 23 août 2014.

En dehors des experts en cybersécurité qui mettent en avant l'absence de mesures de sécurité des outils numériques, peu d'acteurs publics dont les élus ont pris la mesure de ces différents risques. A Nice, le maire s'est par exemple montré démuni face à la révélation de failles de sécurité dans un système de paiement de parking par carte bancaire via une application[5].

Face à ces diverses menaces, il existe un large panel de solutions techniques fortement recommandées voire obligatoires dans le cadre de la sécurité des systèmes d'information, à l'instar des mesures de contrôle d'accès, de cloisonnement des réseaux ou encore de chiffrement des données et plus largement d'analyse de risques[6]. Au sein de l'Union européenne, ces mesures techniques et organisationnelles sont appuyées par un cadre réglementaire de plus en plus riche, mêlant progressivement à la sécurité des infrastructures, la protection des « services » ou des données elles-mêmes. De manière non-exhaustive, il en est ainsi de la directive NIS (« *Directive on security of network and information systems* »[7]) qui oblige les Opérateurs de Services Essentiels (OSE) à sécuriser leurs infrastructures et services considérés comme « critiques »[8]. Le Règlement général pour la protection des données à caractère personnel incite par ailleurs les acteurs publics comme privés à mener des méthodologies d'analyse d'impact (dites « *PIA* ») concernant les données à caractère personnel[9].

Ce cadre réglementaire hétérogène soulève plusieurs types de questions :

- Quels nouveaux risques la numérisation des services publics urbains fait-elle peser sur le fonctionnement des villes ?
- Quelles sont les responsabilités actuelles des collectivités face à ces risques en matière de cybersécurité ?
- La règlementation relative à la sécurité des systèmes d'information est-elle adaptée aux nouveaux systèmes urbains qui se mettent en place via les objets connectés ?
- *In fine*, les collectivités doivent-elles faire l'objet d'une règlementation particulière en matière de cybersécurité eu égard à leur mission de service public ?

[5] Le Figaro, « Pris de court, Christian Estrosi interrompt une interview », 6 juin 2014.
[6] Voir le Référentiel Général de Sécurité des Systèmes d'information (RGS) : https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.
[7] Directive NIS : https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
[8] Plus récemment encore, le « Cybersecurity Act » enjoint les industriels à certifier les produits et services informatiques qu'ils produisent afin de garantir le respect de normes de sécurité déterminées. Communiqué de presse du Parlement européen, 12 mars 2019.
[9] Article 35 du Règlement général sur la protection des données à caractère personnel.