La cybersécurité : une obligation de service public ?

Antoine Cnudde,
Doctorant en droit public à l'université Paris 2 Panthéon-Assas

Beau cadeau de Saint Valentin, le 14 février dernier, la région Grand Est a été victime d'une cyberattaque de très grande ampleur[1]. Sur plusieurs sites de la collectivité, pas moins de 7 500 agents et 169 élus ont été privés de leur messagerie professionnelle, de leur accès aux serveurs ainsi que de certains logiciels métier. Malgré l'intervention rapide de l'ANSSI[2] et d'un prestataire extérieur, il a fallu travailler plus d'une semaine avant un retour à la normale. Chanceuse dans son malheur, la région affirme n'avoir perdu aucune donnée sensible, notamment financière.

Et si cela avait été le cas ? Les collectivités et autres acteurs publics et parapublics ont en leur possession de nombreuses données, plus ou moins sensibles, notamment à caractère personnel, qui leur sont propres ou qu'ils tiennent de leurs administrés.

Tiers de confiance par excellence, l'entité publique est garante de la sécurité des données qu'elle détient, particulièrement à travers la sécurité de ses systèmes d'information. Cela dit, tous les acteurs publics sont-ils concernés ? Quelles sont les obligations spécifiques de sécurité qui s'imposent à ces entités ? En ont-elles les moyens techniques et financiers ?

S'agissant du périmètre des acteurs concernés par ces obligations particulières, en droit, on connait bien la notion de service public. En premier lieu, c'est une nature. Certaines activités relèvent de la qualification de service public, d'autres non. En deuxième lieu, c'est un régime. Lorsque l'on est en présence d'un service public, certaines règles spécifiques s'appliquent.

Bien évidemment, la grande diversité des activités qui peuvent recevoir la qualification de service public fait qu'il n'existe pas un régime unique et uniforme. Cela étant, certaines grandes règles sont impératives pour tous les services publics. Classiquement, on parle d'« obligations de service public ».

Dans la doctrine administrative classique, on connait trois grandes obligations de service public : égalité, continuité et mutabilité. C'est de ces obligations originelles que découlent par exemple l'obligation de laïcité des agents d'un centre hospitalier ou l'obligation pour un opérateur de transports en commun, même juridiquement privé, d'assurer un service minimum, même en cas de grèves.

---

[1] La presse s'est fait échos de cet événement. Voir notamment « La région Grand Est victime d'une cyberattaque d'ampleur », S. Constanzer, *France Bleu*, 20 févr. 2020 ; « La région Grand Est victime d'une cyberattaque massive », C. Domenech, *Capital*, 20 févr. 2020.

[2] Agence nationale de la sécurité des systèmes d'information

En ce qui concerne la cybersécurité, ce périmètre est-il pertinent ? Les normes de sécurité demandées aux personnes en charge d'une mission de service public sont-elles particulièrement renforcées vis-à-vis des acteurs privés ?

La doctrine plus récente tend effectivement à démontrer qu'il existe de nouvelles obligations de service public qui s'imposent aux activités qualifiées comme telles. L'une d'entre elles est l'obligation de sécurité, notamment « cyber ». Cette obligation générale trouve à s'appliquer de manière plus ou moins forte selon les cas.

Matériellement, les règlementations peuvent être spécifiques et différentes si le service ne concerne que l'Administration ou s'il y a interaction avec l'administré. Par exemple, dans le cas spécifique de la mise en place, par l'administration d'un téléservice pour l'administré, le référentiel général de sécurité (RGS)[3] et le règlement « eIDAS »[4] s'imposent.

En outre, selon un critère organique, l'obligation de sécurité sera plus ou moins contraignante et stricte selon le type de service. On distingue par exemple les « opérateurs d'importance vitale » (OIV) ou les « opérateurs de services essentiels » (OSE).

Le traitement de ces questions à l'occasion des ateliers de *Convergences du droit et du numérique* semble tout indiqué. En effet, sans un cahier des charges précis (c'est-à-dire sans la technique) difficile de produire des règles pertinentes et efficaces. De plus, l'implémentation de ces règles demande également à confronter la technique informatique à la réalité de l'Administration et du périmètre de son action.

[3] Référentiel pris en application du décret n° 2010-112 du 2 février 2010, lui-même pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[4] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil, 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (Règlement eIDAS).