LE TEMPS

FORUM ABONNÉ

Protection (et fuites) des données: quelle responsabilité pour les collectivités?

OPINION. Les cyberattaques subies par les communes de Rolle et Montreux illustrent les risques de fuites de données encourus par les administrations publiques. Or elles n'y sont souvent pas préparées, et l'arsenal législatif actuel ne leur fournit pas les outils nécessaires pour y remédier

La commune de Montreux, victime d'un hacking, 2 juillet 2021. — © Valentin Flauraud/EPA v

Alexandre Jotterand, avocat, étude Id Est avocats Sàrl

Publié lundi 25 octobre 2021 à 19:41
Modifié mardi 26 octobre 2021 à 10:58

A l'instar des entreprises privées, les administrations publiques traitent toujours plus de données personnelles. Outre les données usuelles, telles que le nom, la date de naissance et les coordonnées, certaines informations peuvent revêtir un caractère sensible: extraits de poursuites, jugements civils ou pénaux, ou encore relevés fiscaux.

Alexandre Jotterand, avocat, étude Id Est avocats Sàrl. DR

Tout cela impose que ces données soient gérées de manière rigoureuse. Or, les collectivités ne disposent souvent ni des processus nécessaires, ni des mesures de sécurité adéquates pour en assurer une saine gestion, ce qui en fait des cibles de choix pour des acteurs malveillants.

Lire aussi: Des signaux d'alerte avaient précédé la cyberattaque de Rolle

Prendre des mesures correctives

Des mesures correctives doivent donc être prises rapidement afin d'accroître la sécurité des infrastructures informatiques et d'intégrer la protection des données personnelles dans l'ADN des collectivités (selon le principe du *privacy by design*). Malheureusement, le corpus législatif actuel, qui est morcelé et souvent dépassé, ne fournit pas les bonnes incitations.

Il n'y a pas de cadre légal unifié. Il existe bien une loi fédérale sur la protection des données (LPD), qui a été entièrement mise à jour en septembre 2020 (avec une entrée en vigueur prévue en 2023), mais elle ne s'applique qu'aux entreprises privées et aux administrations publiques fédérales. Fédéralisme oblige, les administrations cantonales et communales sont soumises, elles, aux lois édictées de manière souveraine par chaque canton. Toutes ces législations cantonales doivent aujourd'hui être révisées et les cantons accusent un retard important sur ce front. Cela complique le travail des collectivités, qui ne savent pas exactement quelles exigences leur seront applicables à l'avenir.

Lire également: La cybersécurité, condition-cadre pour une Suisse attractive

Des exigences lacunaires

A l'heure actuelle, les exigences posées par les législations cantonales et fédérales sont souvent lacunaires: les administrations sont par exemple tenues de sécuriser les données personnelles qu'elles traitent, mais elles n'ont pas l'obligation légale de communiquer en cas de fuite de données.

Il en découle un décalage entre la responsabilité morale (ou réputationnelle) des collectivités, qui doivent satisfaire aux attentes de la collectivité, et leur (faible) responsabilité juridique. Cette problématique est exacerbée par le manque de moyens à disposition des autorités chargées de l'application de la loi, qui se limitent le plus souvent à l'établissement de simples recommandations.

La situation est différente dans l'Union européenne, où les collectivités publiques peuvent être lourdement amendées. A titre d'exemple, l'autorité italienne de protection des données a infligé en juillet 2021 une amende de 800 000 euros à la municipalité de Rome pour plusieurs manquements constatés en lien avec son système de parcomètres, sanctionnant notamment une sécurisation insuffisante des données personnelles.

Si le système européen est probablement excessif à bien des égards, il a conduit à une prise de conscience de l'importance de la protection des données personnelles, y compris en Suisse. Or, cet objectif implique de doter les autorités chargées de l'application de la loi des moyens nécessaires pour assurer leur mission, ce qui n'est pas le cas pour le moment.

Des révisions nécessaires

Enfin, le cadre législatif ne fournit pas les bonnes incitations. Selon la conception suisse, la violation des règles sur la protection des données est une affaire pénale. Ainsi, la loi fédérale révisée prévoit une amende pouvant atteindre 250 000 francs si les exigences minimales en matière de sécurité des données ne sont pas respectées. Toutefois, ce n'est pas l'entité fautive qui sera poursuivie pénalement, mais la personne physique à qui le manquement pourrait être reproché (p. ex. un directeur ou le responsable de la sécurité informatique). Les employés ne sont d'ailleurs pas tous logés à la même enseigne, puisque ces sanctions pénales ne visent pour l'heure que les employés d'entreprises privées, à l'exclusion des entités publiques. Vu la sensibilité des données traitées par les collectivités, cette distinction privé/public ne semble pas justifiée. De plus, sanctionner uniquement l'individu sans responsabiliser la collectivité pourrait s'avérer contre-productif.

Il reste à voir comment les parlements cantonaux empoigneront la révision de leurs législations sur la protection des données. Contrairement à certaines idées reçues, un cadre légal clair, avec des obligations précises et une surveillance efficace est préférable non seulement pour les administrés, mais également pour les administrations. Rappelons que la responsabilité des administrations en lien avec la gestion des données personnelles n'est pas uniquement juridique, mais également morale. Tout déséquilibre (dans un sens ou dans l'autre) entre ces différentes responsabilités complique le travail des administrations, au risque d'éroder la confiance des administrés.