



DÉCISIONS RÉCENTES DE LA CNIL : QUEL IMPACT POUR LES COLLECTIVITÉS ?

Par David Conerardy, avocat au cabinet Seban & Associés

■ Existe-t-il un mouvement général de renforcement des contrôles de la Cnil ?

Lorsque l'on étudie les informations à notre disposition (décisions publiées ou informations disponibles en open data), on constate un mouvement général de renforcement des sanctions infligées par la Cnil (Commission nationale de l'informatique et des libertés). Pour l'année 2017, il y a eu 342 contrôles Cnil pour 14 saisies de la formation restreinte. Les contrôles ont eu pour fondement la loi informatique et libertés dans 296 cas et la vidéosurveillance dans les 46 cas restants. Pour ce qui est des saisies de la formation restreinte, il y a eu 5 avertissements pour 9 sanctions (publiques et non publiques). Sur 342 contrôles de la Cnil, 82 ont concerné des acteurs publics ou parapublics (soit 23,97 % du total).

Pour l'année 2018, nous n'avons pas encore l'ensemble des données qui seront publiées en open data courant juin 2019. Toutefois, nous avons à notre disposition les chiffres relatifs aux sanctions pécuniaires publiques. Ils montrent une hausse des sanctions pécuniaires publiques par rapport à 2017 (passage de 6 à 9 sanctions), avec une très nette augmentation du montant moyen des amendes (multiplication par 3,65) avec un record à 400 000 € (2,67 fois supérieur au dernier record de 2017).

■ Les acteurs publics ont-ils été concernés par cette hausse en 2018 ?

Le détail des organismes sanctionnés en 2018 montre la sanction de plusieurs associations d'intérêt général et organismes publics. Si la sanction de l'OPH de Rennes peut paraître conjoncturelle (détournement des finalités à des fins supposément politiques), les deux associations ont été sanctionnées pour des motifs plus

habituels : les manquements à leurs obligations de sécurité des données.

Ce renforcement des sanctions doit néanmoins se lire sous le prisme de leurs situations d'espèce. Les contrôles ont été réalisés après que des individus ont informé la Cnil des manquements et non pas à la suite de contrôles délibérés. L'année 2018 a montré que les organismes publics et parapublics, s'ils ne sont pas ciblés délibérément par le service des contrôles, ne bénéficient plus de la clémence de la Cnil. Le montant des sanctions montre bien que les organismes publics ne sont pas considérés comme des structures à part mais bien comme des responsables de traitement comme les autres.

■ Sur quel point faut-il être particulièrement attentif ?

Depuis 2018, les acteurs traitant des données doivent être plus attentifs aux questions de sécurité. La protection des données à caractère personnel est la source de 7 des 9 sanctions publiques de 2018. Il est clair que la Cnil, si elle proportionne toujours la sanction aux nombres de personnes concernées et à la nature des données publiées, risque d'être de plus en plus dure sur cette thématique.

■ Les collectivités sont-elles concernées ?

Les problématiques de sécurisation des données sont aussi réelles pour une entreprise privée que pour un organisme public. Il n'y a rien qui justifie aujourd'hui une plus grande clémence de la Cnil envers les acteurs publics dans la protection des principes essentiels du RGPD (règlement général sur la protection des données). On peut même penser que les sanctions seraient tout aussi élevées en raison de la nature des données collectées, souvent plus sensibles que celles obtenues par des opérateurs privés.

De même, les manquements aux obligations d'information et les méthodes de recueil du consentement, lorsque celui-ci est le fondement légal du traitement d'une collectivité, sont susceptibles d'être sanctionnés aussi fermement, et ce notamment au regard des rappels réguliers et continus de la Cnil sur le sujet. Les acteurs locaux ne pourront plus arguer de leur méconnaissance du cadre législatif pour minorer une éventuelle violation des dispositions du RGPD.

■ Qu'en est-il en 2019 ?

Le mois de décembre 2018 et le début d'année 2019 ont été marqués par une accélération des sanctions de la Cnil. Cela s'explique par la fin du deuxième mandat de la présidente Falque-Pierrotin et le remplacement d'une partie du collège de la Cnil.

Concernant les sanctions, en décembre 2018, la formation restreinte a prononcé deux amendes de 400 000 € pour Uber France et 250 000 € pour Bouygues Telecom en raison de problèmes relatifs à la sécurité des données collectées. En février 2019, la Cnil a prononcé une amende record de 50 M€ contre Google LLC en raison d'une violation du RGPD, entré en vigueur le 25 mai 2018. Il s'agit de la première sanction en France sur un tel fondement et la plus élevée jamais prononcée en Europe.

■ En quoi consiste cette sanction record ?

Tout d'abord, la formation a estimé qu'il y avait une violation continue des obligations de transparence et d'information (article 12 du RGPD) lors de la collecte des données personnelles (article 13 et 14 du RGPD) et que les droits des personnes n'étaient pas assez clairement indiqués (article 15 à 22 du RGPD). En effet, la formation restreinte a constaté que les informations essentielles (finalité, durée de

conservation ou catégories de données) étaient anormalement disséminées dans de multiples espaces. Ensuite, la formation restreinte de la Cnil a sanctionné l'absence de base légale pour les traitements de personnalisation de la publicité.

Il existe six bases légales (article 6 du RGPD) qui permettent de justifier de la licéité d'un traitement, et seules deux pouvaient être utilisées par la société : le consentement des utilisateurs et l'intérêt légitime de l'entreprise. Il ressort de la décision que ces deux bases légales étaient utilisées indistinctement par Google sans que la clarification ne soit portée à la connaissance des utilisateurs.

■ Que tirer de cette décision pour les collectivités ?

La formation restreinte a fait le choix de sanctionner alors même que la violation ne concernait pas des données sensibles (au sens de l'article 9 du RGPD) et qu'aucune mise en demeure n'avait été préalablement envoyée à Google LLC. Ces éléments laissent sous-entendre que les agents chargés du contrôle et des sanctions seront moins compréhensifs dans le futur. De plus, le fondement des sanctions n'étant pas un fondement de nature à concerner plus spécifiquement les acteurs privés que publics, il n'est pas impossible qu'un usager du service public ou un administré décide de saisir la Cnil contre un acteur local public ou une collectivité. Si ce cas devait déclencher un contrôle de la Cnil,

il n'est pas sûr qu'elle soit plus clémentement si elle découvre que la sécurité des données n'est pas assurée ou que des mentions d'information ne sont pas régulièrement transmises aux administrés.

■ Les acteurs publics n'ont-ils pas des latitudes ?

En réalité, certains éléments permettent de penser que les collectivités ont encore des marges de manœuvre. Pour les nouvelles obligations ou les droits issus du RGPD (droit à la portabilité ou analyses d'impact), les contrôles opérés auront essentiellement pour but d'accompagner les organismes publics vers une bonne compréhension et la mise en œuvre opérationnelle des textes. On peut légitimement penser que la Cnil aura une approche plus clémentine sur toutes ces obligations nouvelles. Ensuite, il existe un certain nombre d'obligations issues du RGPD qui paraissent moins concerner les collectivités. Par exemple, l'absence d'observation du cadre juridique du transfert de données vers l'international ou encore l'exercice du droit à la portabilité.

Enfin, l'ampleur de la sanction infligée à Google ne paraît pas transposable à une collectivité. En effet, la notion de chiffre d'affaires annuel mondial n'a pas de sens pour une collectivité (de sorte qu'elle est soumise aux plafonds de 10 et 20 M€), et on peut légitimement penser que c'est la qualité de géant de Google qui a poussé la Cnil à frapper aussi fort. ●

Changement de gouvernance au sein de la Cnil

Le collège de la Cnil, composé de 18 membres, a été partiellement renouvelé en février dernier et s'est réuni le 14 février pour procéder aux élections du vice-président délégué et des membres de la formation restreinte. La nouvelle présidente, Marie-Laure Denis, a été désignée pour diriger la Cnil les cinq prochaines années et devra impulser une nouvelle dynamique ainsi que sa vision en matière de données à caractère personnel.