PROTECTION DES DONNÉES

Le renforcement des sanctions administratives de la Cnil guette les collectivités

Décembre 2018 et janvier 2019 ont vu l'adoption d'amendes record par la Cnil pour des manquements à la loi informatique et libertés et au règlement général sur la protection des données (RGPD), semblant annoncer la fin de la période transitoire, au moins sur les principes fondamentaux. Comme toute personne morale manipulant les données personnelles, les collectivités peuvent faire l'objet de lourdes sanctions.

1 L'ADOPTION RECORD DE SANCTIONS ADMINISTRATIVES

Sanctions pour défaut de sécurité des données : Bouygues et Uber épinglés

Dans deux délibérations rendues successivement le 20 et 26 décembre 2018, la formation restreinte de la Commission nationale de l'informatique et des libertés (Cnil) a prononcé deux amendes administratives de respectivement 400 000 euros pour Uber France et 250 000 pour Bouygues Telecom en raison de problèmes relatifs à la sécurité des données collectées. Dans le cas de l'opérateur téléphonique, une vulnérabilité liée à un défaut de sécurité permettait d'accéder à des contrats et factures de deux millions de clients B&You pendant plus de deux ans. L'entreprise, une fois qu'elle l'a su, a corrigé rapidement la faille de sécurité mais la formation restreinte de la Commission a considéré que la société avait manqué à son obligation d'assurer la sécurité des données personnelles et ce d'autant plus que le défaut de sécurité avait pour origine une erreur d'un agent de la société (la fonction d'authentification sur l'espace client avait été désactivée pour une phase de test et jamais réactivée).

Dans le cas d'Uber, la société a révélé dans la presse avoir été victime en 2016 d'une violation de sécurité avec le vol de données personnelles de près de 57 millions d'utilisateurs, dont 1,4 million de Français. Comme dans la situation de Bouygues Telecom, la formation restreinte de la Cnil a estimé que cette attaque n'aurait pu aboutir si des mesures élémentaires de sécurité avaient été mises en place, comme imposer une authentification forte pour ses ingénieurs sur la plateforme de développement « Github » ou encore en stockant de manière chiffrée les informations présentes au sein du code source de celle-ci.

La Cnil très vigilante sur les défauts de sécurité des systèmes d'information

Ces deux décisions sont très instructives pour l'ensemble des responsables de traitement, qu'ils soient publics ou privés. Déjà, la formation restreinte de la Cnil aurait pu faire le choix de mettre préalablement les deux sociétés en demeure afin qu'ils respectent leurs obligations de sécurité et ne pas sanctionner leur comportement par une amende administrative. Ensuite, les montants des sanctions sont bien supérieurs à ce qui était décidé jusqu'alors par la formation restreinte pour des manquements similaires. Enfin, ces deux décisions montrent que la Cnil reste particulièrement vigilante sur ce qui touche à la sécurité des systèmes d'information et n'hésite pas à sanctionner les manquements, plusieurs années même après la connaissance et la matérialisation de la violation de données personnelles.

« L'exemple » Google

Dans une décision rendue le 15 janvier 2019, la Cnil a prononcé une amende record de 50 millions d'euros 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. Le RGPD a institué un mécanisme de « guichet unique » qui prévoit qu'un organisme établi dans l'Union européenne peut avoir pour interlocuteur principal l'autorité du pays où il a son établissement principal.

La Cnil, pour établir que le système du guichet unique du RGPD n'était pas applicable, a considéré que le siège européen de Google (situé en Irlande) ne disposait pas d'un pouvoir de décision suffisant sur les traitements mis en œuvre au travers du système d'exploitation Android et de la configuration d'un téléphone mobile. De ce fait, comme le pouvoir de décision était détenu par Google LLC (située aux Etats-Unis), toutes les autorités de protection des données à caractère personnel étaient compétentes pour prendre des sanctions concernant les traitements mis en œuvre par cette entreprise.

Après avoir constaté qu'elle était bien compétente, la formation restreinte de la Cnil a relevé deux séries de manquements au RGPD.
Dans un premier temps, la formation a estimé qu'il y avait une violation continue des obligations de transparence et d'information (art. 12 du RGPD) lors de la collecte des données personnelles (art. 13 et 14) et que les droits des personnes n'étaient pas assez clairement indiqués (art. 15 à 22).
En effet, la formation restreinte a constaté, au moment des investigations, que les informations essentielles (finalité, durée de conservation ou catégories de données) étaient anormalement disséminées dans de multiples espaces où il était nécessaire d'activer des boutons ou onglets pour prendre connaissance des informations complémentaires. De plus, la Cnil a remarqué que les informations fournies n'étaient pas suffisamment claires ou compréhensibles par rapport aux aspects intrusifs des différents traitements et que les finalités étaient trop génériques et vagues.

La sanction pour manquement aux obligations d'information

Dans un second temps, la formation restreinte de la Cnil est venue sanctionner l'absence de base légale pour les traitements de personnalisation de la publicité. Il existe six bases légales (art. 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 au traitement et l'intérêt légitime de l'entreprise. Il ressort de l'instruction des agents de la Cnil que ces deux bases légales étaient utilisées indistinctement par Google sans que la clarification ne soit portée à la connaissance des utilisateurs.
La formation restreinte de la Cnil a reproché à la société américaine de ne pas recueillir valablement le consentement des personnes pour les traitements de personnalisation de publicité alors que l'intérêt légitime ne pouvait être une base légale retenue pour ces traitements.
La formation a d'ailleurs profité de cette décision pour rappeler que la dispersion des informations sur plusieurs espaces et documents (en plus de présenter des cases précochées au moment de la collecte) ne pouvait constituer un consentement éclairé, spécifique et univoque.
Le montant de 50 millions d'euros représente actuellement la plus lourde sanction européenne en matière de données personnelles.

2 UN COUP DE SEMONCE À NE PAS NÉGLIGER PAR LES COLLECTIVITÉS

Si ces sanctions peuvent paraître abstraites pour les acteurs publics, elles sont pourtant riches d'enseignements qu'il ne faut pas négliger sous peine de voir les organismes publics sanctionnés à leur tour.

Fin annoncée de la clémence au regard du caractère sensible des données

Les problématiques de sécurisation des données sont aussi réelles pour une entreprise privée que pour un organisme public, et il n'y aurait rien qui justifierait aujourd'hui une plus grande clémence de la Cnil envers les acteurs publics dans la protection des principes essentiels du RGPD. On peut même penser que les sanctions seraient tout aussi élevées en raison de la nature des données collectées qui sont 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, de bonne foi, arguer de leur méconnaissance du cadre législatif pour minorer une éventuelle violation des dispositions du RGPD.
Dans les cas particuliers des sanctions d'Uber et de Bouygues Telecom, la formation restreinte a fait le choix de sanctionner les entreprises alors même que la vio- ●●●

Les élections européennes et l'ouverture des campagnes municipales risquent d'être des moments ciblés par le service des contrôles de la Cnil pour s'assurer du respect du RGPD.

La fin de la période transitoire

Il semble que la période transitoire admise explicitement par la Cnil tende à se terminer. Dans un entretien accordé à « Contexte » le 19 juin 2017 Isabelle Falque-Pierrotin, alors présidente de la Cnil, indiquait qu'il ne fallait pas voir « le RGPD comme un couperet en 2018 » et qu'il fallait « déconstruire cette idée qu'il y aura un coup de tonnerre en mai 2018 et que, comme des petits soldats, il faut que les entreprises soient prêtes à 100 % ». Cependant, presque trois ans après l'adoption du RGPD et neuf mois après son entrée en vigueur, il semble assez clair que la Commission ne laisse plus passer les méconnaissances basiques des dispositions du règlement européen et de la loi relative à l'informatique, aux fichiers et aux libertés.

RÉFÉRENCES

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit RGPD
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi informatique et libertés

lation ne concernait pas des données sensibles (au sens de l'art. 9 du RGPD), qu'elles avaient promptement réagi et qu'aucun préjudice n'avait été causé aux personnes concernées. Ces éléments auraient légitimement pu infléchir la décision de la formation restreinte.

Ce point, associé au choix de ne pas mettre en demeure les organismes poursuivis, laisse 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, par essence, un fondement de nature à concerner plus spécifiquement les acteurs privés que publics, il n'est pas impossible qu'un usager du service public décide de saisir la Cnil contre un acteur local public ou une collectivité territoriale. Si ce cas devait déclencher un contrôle de la Commission, il n'est pas sûr qu'elle se comporte avec plus de clémence 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.

L'évaluation prospective avec les municipales en ligne de mire

L'année 2019 risque d'être une année où le comportement des organismes publics sera plus scruté par les agents de la Cnil qu'il ne l'a été par le passé. Les élections européennes et l'ouverture des campagnes municipales risquent d'être des moments ciblés par le service des contrôles de la Commission pour s'assurer que les manquements « habituels » à la loi informatique et liberté ne seront pas répétés maintenant que le RGPD est entré en vigueur. Cette situation est d'autant plus vraie que l'année 2018 a déjà vu la condamnation d'organismes publics œuvrant pour l'intérêt général, à l'instar de l'Association pour le développement des foyers et l'Office public de l'habitat de Rennes (1). Par ailleurs, les premières sanctions européennes sur le fondement du RGPD ont concerné un centre hospitalier portugais (2).

Les obligations nouvelles observées avec mansuétude ?

Toutefois, certains éléments nous permettent aussi de penser que les collectivités ont encore différentes marges.Déjà, pour les nouvelles obligations ou les nouveaux droits issus du RGPD (tels que le droit à la portabilité ou les 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, si elle décide de sanctionner plus rigoureusement les manquements les plus évidents au RGPD, aura une approche plus clémente sur toutes ces obligations nouvelles. Ensuite, il existe un certain nombre d'obligations issues du RGPD qui paraissent moins concerner les collectivités territoriales. 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 territoriale. En effet, la notion de chiffre d'affaires annuel mondial n'a pas de sens pour une collectivité territoriale (de sorte qu'elle est soumise aux plafonds de 10 et 20 millions d'euros), et on peut légitimement penser que c'est la qualité de géant du Net de Google qui a poussé la Cnil, en accord avec les autres régulateurs européens, à frapper aussi fort.

(1) L'association a été condamnée à une amende de 75 000 euros pour atteinte à la sécurité des données de demandeurs de logement et l'OPH de Rennes à payer 30 000 euros pour une utilisation du fichier des locataires incompatible avec la finalité initiale.

(2) Le 19 octobre 2018, l'équivalent portugais de la CNIL a condamné l'hôpital de Barreiro à une amende de 400 000 euros pour des manquements au principe d'intégrité et de confidentialité des données de santé des patients alors que leur accès n'était pas strictement limité aux personnes chargées du suivi médical.

Par David Conerardy et Aloïs Ramel,
avocats à la cour, SCP Seban et Associés