

<https://www.observatoire-collectivites.org/spip.php?article6695>

Traitement des données personnelles pour la gestion du personnel dans les collectivités territoriales : incidence du défaut d'information des agents sur la légalité des sanctions



disciplinaires

Publication date: mercredi 28 décembre 2016

- Jurisprudence -

Copyright © Observatoire Smacl des risques de la vie territoriale - Tous

droits réservés

Un agent refusant de se soumettre à un système de pointage impliquant un traitement de ses données personnelles (ici un contrôle biométrique) peut-il être sanctionné disciplinairement même en l'absence d'information individuelle préalable sur l'existence d'un tel dispositif comme l'impose pourtant la loi "Informatique et libertés" ?

Oui : les obligations d'information de la commune, en tant que responsable du traitement de données personnelles, prévues par l'article 32-1 de la loi du 6 janvier 1978, modifiée dite loi "Informatique et libertés", ne sont relatives qu'aux modalités concrètes de fonctionnement du traitement, et leur méconnaissance ne peut avoir, à elle seule, pour effet de rendre la décision administrative instaurant ce traitement inopposable aux personnes concernées par le recueil de données personnelles. En l'espèce, une commune avait pris deux sanctions disciplinaires (un avertissement et une exclusion temporaire de fonction de deux jours) à l'encontre d'un agent ayant refusé de se soumettre au contrôle biométrique de son temps de présence. L'agent avait obtenu l'annulation des sanctions, les juges d'appel estimant que l'absence d'information individuelle avait eu pour effet de rendre le dispositif inopposable aux agents. Le conseil d'Etat censure cette position et donne raison à la commune. A noter que depuis une délibération de la CNIL de septembre 2012 il n'est plus possible de mettre en place un contrôle biométrique pour le contrôle du temps de présence des agents et salaires, ce procédé étant jugé disproportionné par rapport à l'objectif poursuivi. L'employeur peut en revanche toujours mettre en place des outils – y compris biométriques – de contrôle individuel de l'accès pour sécuriser l'entrée dans les bâtiments, ou dans les locaux faisant l'objet d'une restriction de circulation. L'arrêt du Conseil d'Etat (non

publié au recueil Lebon) n'en reste pas moins transposable à tous les traitements de données à caractère personnel mis en œuvre par les collectivités pour la gestion de leur personnel.

En octobre 2010, le maire d'une commune (40 000 habitants) décide, par arrêté, la création d'un traitement de données à caractère personnel, reposant sur un dispositif biométrique de reconnaissance des contours de la main, dont l'objet est la gestion des horaires et des temps de présence des agents municipaux. Régulièrement déclaré auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) [1], ce traitement n'a cependant pas donné lieu à une information préalable et individuelle des agents, comme l'exige pourtant l'article 32-I de la loi du 6 janvier 1978 modifiée, dite loi Informatique et libertés. L'un d'eux refuse de se soumettre à ce contrôle et fait l'objet de deux sanctions disciplinaires (un avertissement et une exclusion temporaire de fonction de deux jours). Il conteste la légalité de ces sanctions sur la base du défaut d'information individuelle et préalable.

L'agent est débouté en première instance. Pour faire droit à sa demande, la cour administrative d'appel relève que le système biométrique n'a fait l'objet d'une information individuelle que deux années après le prononcé des sanctions [2]. Or, si le défaut d'information exigée par l'article 32-I de la loi Informatique et libertés « est sans incidence sur la légalité de la décision du maire d'instaurer un dispositif biométrique, sa méconnaissance doit en revanche être regardée comme ayant eu pour effet de rendre une telle décision inopposable aux agents de la commune ». L'arrêté du maire reste donc légal mais il est inopposable aux agents. Les sanctions en découlant doivent par conséquent être annulées.

Sur pourvoi de la commune, le Conseil d'Etat confirme qu'il incombe au responsable d'un traitement de données à caractère personnel de fournir à toute personne concernée par l'inscription de données dans ce traitement, dès leur enregistrement, l'ensemble des informations prévues au I de cet article 32 de la loi du 6 janvier 1978, y compris quand ces données personnelles ne sont pas recueillies auprès de la personne directement concernée elle-même.

Mais pour autant c'est à tort, poursuit le Conseil d'Etat, que les juges d'appel en ont déduit que le dispositif était inopposable aux agents. En effet :

"les obligations du responsable du traitement de données ne sont toutefois relatives qu'aux modalités concrètes de fonctionnement de ce dernier et leur méconnaissance ne peut avoir, à elle seule, pour effet de rendre la décision administrative instaurant ce traitement inopposable aux personnes concernées par le recueil des données personnelles".

C'est donc par erreur de droit que la cour administrative d'appel a estimé qu'une telle méconnaissance devait être regardée comme ayant eu pour effet de rendre la décision du maire de la commune inopposable aux agents de la commune et en déduire que les sanctions litigieuses étaient illégales.

Une manière implicite pour le Conseil d'Etat de souligner qu'il n'existe pas, pour la fonction publique, de pendant aux dispositions de l'article L.1222-4 du code du travail aux termes duquel "aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance" ?

Toujours est-il que cet arrêt du Conseil d'Etat (non publié au recueil Lebon) relatif à l'incidence du défaut

d'information des agents n'en demeure pas moins transposable pour tous les traitements de données à caractère personnel mis en œuvre dans les collectivités pour la gestion de leur personnel. Si le défaut d'information des agents, en l'état de la jurisprudence du Conseil d'Etat, n'a pas pour effet de rendre la décision administrative instaurant ce traitement inopposable aux agents, il est toujours préférable de satisfaire à cette obligation imposée par la loi "Informatique et libertés". Ne serait-ce que pour s'éviter un contentieux...

[Conseil d'État, 28 décembre 2016, NÂ° 384236](#)



PS:

– La création d'un traitement de données à caractère personnel doit faire l'objet d'une information préalable et individuelle des personnes concernées (en l'espèce les agents) portant sur l'identité du responsable de traitement, les finalités poursuivies, le caractère obligatoire ou non des réponses et les conséquences d'un défaut de réponse, les destinataires des données, les droits de la personne et le cas échéant les transferts hors Union européenne.

– Mais le Conseil d'Etat estime que les obligations du responsable du traitement de données ne sont toutefois relatives qu'aux modalités concrètes de fonctionnement de ce dernier et leur méconnaissance ne peut avoir, à elle seule, pour effet de rendre la décision administrative instaurant ce traitement inopposable aux personnes concernées par le recueil des données personnelles.

– Notons que si le contrôle biométrique ne peut plus être mis en œuvre pour le contrôle du temps de présence sur le lieu de travail depuis une délibération de la CNIL de septembre 2012, l'employeur peut en revanche toujours le mettre en œuvre pour sécuriser l'entrée dans les bâtiments, ou dans les locaux faisant l'objet d'une restriction de circulation et ce pour les employés comme pour les visiteurs.

– L'occasion de souligner aussi (source : site de la CNIL) que les traitements de données (notamment biométriques mais pas que), devront être en conformité avec le règlement européen d'ici mai 2018. A cette date, les dispositifs biométriques ne seront plus soumis à l'autorisation préalable de la CNIL. Mais les organismes qui mettent en œuvre ces dispositifs devront en revanche :

- documenter les différentes caractéristiques de leurs traitements être en mesure de démontrer leur proportionnalité ;
- respecter les principes de protection des données par défaut et dès la conception ;
- réaliser une analyse d'impact relative à la protection des données, si leur traitement biométrique est réalisé à grande échelle.

Ces nouvelles exigences sont intégrées dans les autorisations uniques [AU-052](#) et [AU-053](#)

Texte de référence

– [Article 32-I de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés](#)

[– Délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail - décision d'autorisation unique n°AU-007](#)

Etes-vous sûr(e) de votre réponse ?

- [– La publication sur une page Facebook d'un commentaire injurieux à l'égard d'un élu, en dehors des heures de travail, peut-elle justifier la révocation d'un agent ?](#)
 - [– L'employeur peut-il, en l'absence du salarié, contrôler les fichiers présents sur l'ordinateur professionnel mis à sa disposition ?](#)
 - [– Un employeur peut-il hors la présence d'un salarié contrôler le contenu d'une clef USB personnelle connectée à un ordinateur professionnel ?](#)
-

[1] A noter : l'autorisation unique de la CNIL relative à la mise en œuvre d'un dispositif biométrique pour le contrôle du temps de présence sur le lieu de travail a été abrogée le 27 octobre 2012. Ce moyen de contrôle étant considéré comme disproportionné au vu de la finalité.

[2] La CNIL avait d'ailleurs attiré l'attention du maire, à deux reprises, sur l'obligation d'information des agents concernés.