SIAAP

Service public de l'assainissement francilien

Paris, le 12 AOUT 2021

Le Directeur Général

Cher-e-s Collègues,

Des organisations syndicales ayant interpellé le Président du SIAAP par le biais d'un message diffusé à tous (on cherchera où se situe la censure de l'information dénoncée depuis des mois !), il m'apparait légitime de vous informer directement sur le sujet évoqué.

Des explications sont demandées sur un article paru dans un blog[i] de M.Laimé relatif à l'audit de sécurité confié à l'entreprise Ernst et Young.

Le fait même que ce blogueur ait eu accès à cet audit révèle, hélas, la volonté de nuire qui motivent toujours certaines personnes du SIAAP et explique, par conséquent, la demande du Conseil d'Administration de sécuriser toutes informations et toutes données, propriété de l'entreprise publique.

En effet, lors de la séance du Conseil d'Administration du 30 mai 2018[ii], des administrateurs interpellent la direction générale sur les explications qu'elle a à donner sur « les fuites dans la presse » et « sur les mesures de sécurité qui sont prises ou vont être prises pour assurer la sécurité des données ». La directrice générale adjointe en charge des ressources, responsable à cette époque du système d'information, informe des mesures prises en date du 30 mai 2018, et fait part de la possibilité de lancer un audit externe sur le sujet.

Un marché est confié à l'entreprise Ernst et Young en décembre 2018 dans le cadre d'un MAPA, pour les prestations suivantes : audit de sécurité, recherches et investigations de toutes nature afin de cerner, évaluer et identifier les éventuelles failles.[iii]

L'objet du contrat (cf note iii de bas de page) est clair ! Il porte sur la collecte de renseignements et le croisement des données obtenues afin de déterminer les moyens les plus efficaces pour sécuriser les informations de la collectivité et leur non divulgation à l'extérieur.

Il n'y a donc eu et il n'y a aucune de demande d'espionnage de qui que ce soit. Peut-être faut-il simplement rappeler le contenu de la Charte d'utilisation des ressources informatiques et de communication établie en 2017, et notamment son paragraphe 2.1.2[iv].

2, rue Jules César - 75589 Paris Cedex 12 - Tél : 01 44 75 44 20 / 21 - Fax : 01 44 75 44 19

Il est d'ailleurs tout à fait légal pour un employeur d'opérer des contrôles de sécurité de son système d'information par la vérification ponctuelle ou constante des messages entrants comme sortants, qui n'ont pas de caractère personnel et confidentiel, afin de s'assurer de la protection, vis-à-vis de l'extérieur, de la diffusion de ses propres données et également de vérifier l'usage normal des moyens de communication mis à disposition de ses agents. La jurisprudence du Conseil d'Etat est constante en la matière et a été réitérée encore par un arrêt de 2014.

Le SIAAP est donc tout à fait fondé, au vu du corpus réglementaire et législatif et de sa propre charte informatique, à vérifier les comportements de ses agents et le respect de leur obligation de discrétion professionnelle et d'un usage normal des outils d'information dont ils disposent dans le seul but d'exercer leur mission de service public.

Ces vérifications en matière de sécurité, nécessaires au contrôle du respect des obligations statutaires de ses agents, peuvent être effectuées en interne par une personne ou un service ou par une entreprise extérieure chargée d'une telle prestation technique, via un marché public

Pour autant, et pour mettre à bas cette diffamation, il aurait suffi à l'intersyndicale des trois d'interroger le « Correspondant Informatique et Libertés » de l'époque et maintenant le « Délégué à la protection des données », pour savoir si à quelque moment que ce soit une demande de surveillance des boites aux lettres et ordinateurs d'agents a été demandée par la direction générale !

Mais bien évidemment, si cela n'a pas été fait et le grand ramdam orchestré, chacun comprendra que dans la période présente, il ne s'agit pas d'une quelconque défense des intérêts des salariés du SIAAP, mais de régler des comptes.

Je vous prie de recevoir, Cher-e-s Collègues, mes salutations les plus cordiales.

Le Directeur Général

Jacques OLIVIER

---

[i] Un blog est un type de site web utilisé pour la publication périodique et régulière **d'articles personnels**, généralement succincts, rendant compte d'une actualité autour d'une thématique particulière. À la manière d'un journal intime, ces articles — appelés billets — publiés par son/ses propriétaire(s) ou son/ses webmaster(s), sont typiquement datés, signés et présentés dans un ordre rétro chronologique, c'est-à-dire du plus récent au plus ancien. Ils permettent à son auteur, appelé blogueur, d'exprimer une **opinion subjective** et sont la plupart du temps ouverts aux commentaires des lecteurs (Wikipédia)

[ii] Procès-verbal du Conseil d'Administration du 30/05/2018 approuvé le 03/07/2018

[iii] Article 1 du CCP du marché 18S0755
Les stipulations du présent Cahier des Clauses Particulières concernent les prestations suivantes :
Audit de sécurité
Audit, recherches, investigations de toutes nature afin de cerner les éventuelles failles

Le titulaire du marché devra, pour réaliser cet audit, effectuer des recherches et des investigations dans les réseaux du Siaap afin de cerner, évaluer et identifier les éventuelles failles.
Pour cela, il devra :

- *prendre connaissance de l'organisation,*
- *prendre connaissance du mode de fonctionnement et de diffusion des informations et des réseaux supports,*
- *prendre connaissance du périmètre de la mission à partir des documents ou informations fournis,*
- *réaliser des entretiens avec la Direction Générale et toutes les personnes désignées par celle-ci et/ ou sélectionnées par le prestataire après accord de la direction générale,*
- *réaliser des investigations sur place et sur pièces (organisation, réseaux...)*
- *effectuer des investigations numériques plus approfondies en fonction des résultats,*
- *réaliser un approfondissement de la mission par investigation poussées dans les réseaux avec recherches par mots clés aboutissant à une analyse juridique et éventuellement des préconisations*
- *effectuer la poursuite des investigations par la collecte de renseignement d'origine source ouverte,*
- *analyser et synthétiser les éléments recueillis,*
- *proposer des points d'avancement de la réalisation de la mission,*
- *restituer par des livrables à chaque étape de la mission,*
- *établir un rapport final qui sera remis au Directeur Général*

[iv] Les fichiers ou correspondances qui ne font pas apparaitre de caractère personnel sont présumés avoir un caractère professionnel, de sorte que le SIAAP peut y avoir accès en dehors de la présence de l'agent. Le supérieur hiérarchique, ou toute personne déléguée par ce dernier, est habilité à consulter les fichiers et messages à caractère professionnel.