Traitement des demandes d'accès aux journaux informatiques

1. De quoi s'agit-il ?

Les établissements, et notamment leurs RSSI, sont susceptibles de recevoir des demandes d'accès aux journaux informatiques, telles que les suivantes :

- Les membres de la section disciplinaire souhaitent s'appuyer sur les journaux informatiques pour instruire un dossier ;
- Le service des affaires juridiques souhaite obtenir des informations sur les traces relatives à un agent donné, afin d'assurer la défense juridique de l'établissement ;
- Un chef de service demande une recherche dans les journaux informatiques à propos de l'un des agents qu'il encadre ;
- Dans le cadre d'une enquête préliminaire, un officier de police judiciaire demande à obtenir des extraits de journaux informatiques ;
- L'UCLAT (Unité de Coordination de la Lutte Anti-Terroriste) réquisitionne le CERT-Renater, qui transmet la demande au RSSI de l'établissement concerné.

2. Que faire ?

2.1. Les préalables à toute demande

En premier lieu, il est nécessaire de s'assurer que les journaux informatiques ont été mis en œuvre dans le respect de la loi « Informatique et Libertés ».

Concrètement, il s'agit de s'assurer que :

- les finalités d'utilisation des journaux informatiques ont été clairement définies ;
- les données collectées sont pertinentes au regard de ces finalités ;
- la durée de conservation effective des journaux est proportionnelle aux finalités et conforme à la réglementation ;
- les journaux font l'objet de mesures de sécurité adéquates, notamment en termes de contrôle d'accès ;
- une information préalable a été diffusée auprès des personnes ;
- les formalités déclaratives préalables ont été effectuées (déclaration à la CNIL ou bien, si l'établissement a désigné un correspondant Informatique et Libertés (CIL), ajout dans le registre interne des traitements).

De plus, dès lors qu'un contrôle individuel de l'utilisation d'internet est envisagé, les instances représentatives des personnels doivent être préalablement consultées.

Il est recommandé que l'information des personnes soit suffisamment détaillée et couvre les finalités, les catégories de données collectées, la durée de conservation, les destinataires. Ces informations ont vocation à figurer dans la **politique de gestion des traces de l'établissement**, diffusée à tous les usagers et relayée par la charte de bon usage des systèmes d'information. Un exemple de politique type, conforme aux préconisations de la CNIL, est en ligne sur le site du CRU [1].

2.2. L'examen spécifique de la demande

Il convient de distinguer trois cas :

- les demandes issues de services internes à l'établissement,

- les communications à des organismes tiers considérés comme destinataires légitimes,
- les requêtes émises par des tiers autorisés.

2.2.1. Les demandes formulées par les services internes

Selon l'article 3 de la loi « Informatique et Libertés », les services et personnes qui, **en raison de leurs fonctions**, sont chargés de traiter les données personnelles, n'ont pas à figurer dans la déclaration du traitement en tant que destinataires.

Ces personnes incluent évidemment les administrateurs système et réseau et la chaîne fonctionnelle SSI.

De plus, si la politique de gestion des traces cite comme finalité la détection des usages abusifs (contraires aux lois, au règlement intérieur de l'établissement ou à la charte de bon usage des systèmes d'information), alors le service juridique ou les membres des sections disciplinaires peuvent de manière légitime recevoir ponctuellement communication d'extraits des journaux informatiques.

En dernier lieu, il convient de rappeler que toute personne dispose d'un droit d'accès aux données personnelles la concernant.

2.2.2. Les communications à des destinataires légitimes

Les destinataires légitimes figurent dans la déclaration du traitement, telle qu'effectuée auprès de la CNIL ou du CIL de l'établissement.

A titre d'exemple, le CERT-Renater peut être considéré comme destinataire légitime dans le cas de l'analyse d'incidents de sécurité. Il doit alors figurer dans la déclaration du traitement.

2.2.3. Les requêtes émises par des tiers autorisés

La CNIL recommande que toute demande d'accès ou d'analyse des journaux informatiques soit réalisée **par écrit**, compte tenu de l'obligation de sécurité inscrite dans la loi « Informatique et Libertés ». Si l'établissement est réquisitionné par oral, il lui est conseillé de demander un écrit intitulé « *Réquisition judiciaire* » ou « *Demande d'informations dans le cadre de l'exercice du droit de communication prévu par l'article… du Code…* », citant le texte fondant le droit à communication.

Bien entendu, l'établissement doit s'assurer de l'identité et de la qualité du demandeur[1].

La demande doit être ponctuelle et ne peut porter sur l'intégralité d'un fichier.

La liste des principaux tiers autorisés à obtenir communication de données personnelles détenues par les établissements figure dans les documents publiés par la CNIL [2] [3].

2.3. Le traitement de la demande

La transmission des extraits de journaux doit être réalisée de manière sécurisée : chiffrement des données ou remise en main propre des documents ou supports numériques demandés.

[1] Le fait, pour un responsable du traitement, de porter à la connaissance d'un tiers qui n'a pas qualité pour les recevoir des données à caractère personnel, dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, constitue une infraction pénale punie de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-22 du code pénal).

Documents de référence

[1] « Gestion des journaux informatiques » en ligne sur les pages publiques sécurité du CRU, dans la section *Guides et recommandations*
https://www.cru.fr/ssi/securite/index#guides_et_recommandations

[2] Fiche pratique n°16 « Communication à des tiers autorisés d'informations relatives aux personnels et aux étudiants » du *Guide informatique et Libertés pour l'enseignement supérieur et la recherche*, en ligne sur le site de la CNIL
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_CNIL_AMUE_2009.pdf

Pour les établissements ayant désigné un CIL, des documents sont accesibles sur l'extranet de la CNIL (réservé aux CIL après authentification sur http://www.cnil.fr) :

[3] Note sur les tiers autorisés

[4] Note sur les réquisitions judiciaires