université PARIS-SACLAY

1er août 2022

Direction des affaires juridiques et institutionnelles

FICHE

relative à la cyber-surveillance de ses réseaux numériques par l'Université

Cette fiche a pour objet de définir les conditions dans lesquelles l'Université peut ouvrir et prendre connaissance du contenu :
- des fichiers créés par ses personnels et stockés sur les disques durs des ordinateurs mis à leur disposition pour l'exécution du service
- des e-mails envoyés ou reçus par ses personnels au moyen des ordinateurs mis à leur disposition et stockés sur ces machines.

Après avoir évoqué le socle des principes fondamentaux régissant le domaine, il convient de définir, d'abord, les conditions de fond à respecter pour prendre connaissance du contenu, puis l'organisation de la surveillance au sein de l'Université.

I – Les principes fondamentaux

Les règles à appliquer découlent des principes fondamentaux qui suivent.

- ☞ Chacun a droit **au respect de sa vie privée** (Art. 9 du code civil) **et familiale** (Art. 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) du 4 novembre 1950).
- ☞ Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas **justifiées par la nature de la tâche** à accomplir ni **proportionnées au but** recherché (Art. 1121-1 du code du travail).
- ☞ Il incombe à chaque partie de **prouver conformément à la loi** les faits nécessaires au succès de sa prétention (Art. 9 du code de procédure civile)

  Une preuve obtenue en violation du respect de la vie privée est nulle et ne peut être utilisée.
- ☞ La **violation du secret des correspondances** (papier ou e-mail) commise de mauvaise foi est sanctionnée pénalement (Art. 226-15 du code pénal).

II – Les conditions de fond

Il convient de distinguer les documents de nature « *professionnelle* » de ceux de nature « *personnelle* » puis d'examiner les conditions de prise de connaissance ou chacune des catégories.

21 - Sur la distinction entre fichier de nature professionnelle et ceux de nature personnelle

- ☞ Est réputé être « *professionnel* » : tout fichier stocké sur un ordinateur mis à disposition d'un personnel par l'Université ou sur un de ses serveurs, qu'il s'agisse d'un fichier créé par le personnel ou non, d'un simple fichier ou d'un mail adressé ou reçu

par la messagerie interpersonnelle de service mise en place par l'Université ou même d'un message émanant de la messagerie personnelle privée du personnel stocké sur l'ordinateur du service ou le réseau,

sauf :

- les fichiers portant dans leur nom la mention « *personnel* » ou « *privé* » ;
- les mails portant dans leur objet la mention « *personnel* » ou « *privé* » ;
qui deviennent ainsi « *personnels* »

Cette mention « *personnel* » ou « *privé* » est exclusive de toute autre. Ainsi, la simple mention du nom du personnel, ou de ses initiales, ou l'insertion du fichier ou du mail dans un répertoire « *Mes documents* » ne suffisent pas à conférer au document la nature « *personnelle* ».

Il est interdit au personnel de contourner la règle en renommant son disque dur « *Données personnelles* ».

Ces principes valent pour tout matériel, notamment les périphériques de stockage, connectés mêmes momentanément au réseau ou à un ordinateur de l'Université.

22 – Sur les conditions de prise de connaissance du contenu

☞ S'agissant des documents *« professionnels »*

L'Université est autorisée à prendre connaissance du contenu de ces documents numériques **sans conditions particulières et notamment hors la présence de l'intéressé**

☞ S'agissant des documents « *personnels* »

La consultation de ces documents qui est attentatoire au respect de la vie privée n'est possible qu'à plusieurs conditions cumulatives :

- hors risque ou évènement particulier, **la présence de l'intéressé est indispensable** (Cour de cassation) ; à défaut, il suffit qu'il ait été mis en possibilité d'être présent ;

- cette consultation doit être **justifiée par un motif légitime** et **proportionnée au but recherché.**

Concernant le motif légitime, la liste limitative est fixée par l'art. 8 de la CEDH : la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre, la prévention des infractions pénales, la protection de la santé ou de la morale, la protection des droits et libertés d'autrui.

Concernant la proportionnalité, il convient d'exclure toute consultation généralisée et systématique. La consultation doit être strictement limitée au but recherché.

Concernant le risque ou l'évènement particulier, cette condition doit être interprétée de manière très stricte et limitée au cas où le délai nécessaire à la présence de l'intéressé est incompatible avec une consultation immédiate pour des motifs impérieux (présence d'un virus etc.).

L'ensemble de ces règles s'appliquent même si l'Université interdit l'utilisation non professionnelle de l'ordinateur.

III – L'organisation de la cyber-surveillance par l'Université

En application des principes de justification et de motivation précités, il convient de distinguer la surveillance technique de la surveillance intrusive.

31 – La surveillance technique

La surveillance technique a pour objet :
- d'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de Troie etc.) ;
- limiter les risques d'abus de l'utilisation personnelle des réseaux (internet et messagerie de service)

La surveillance technique est de la compétence de l'administrateur du réseau (DSI) dans son travail quotidien sans autorisation particulière de la hiérarchie.

Elle se limite aux opérations suivantes :
- dispositifs de filtrage des sites visités, détection de virus ;
- outils de mesure de la volumétrie des envois.

Elle exclut toute consultation volontaire systématique ou aléatoire de contenus de fichiers ou mails.

En cas de découverte d'éléments mettant en évidence une infraction pénale, un manquement aux règles déontologiques ou un usage non-conforme de l'ordinateur de service, l'administrateur du réseau rend compte à l'autorité de direction compétente aux fins selon les cas :
- de dénonciation de l'infraction en application de l'article 40 du CPP ;
- d'une sanction disciplinaire ;
- de mise en œuvre d'une mesure de surveillance intrusive.

32 – La surveillance intrusive

La surveillance intrusive consiste pour l'administrateur du réseau à prendre, au regard d'un risque identifié, volontairement connaissance du contenu des fichiers ou mails, existant ou à venir, concernant une personnel particulier ou un groupe de personnels particulier ou une ou plusieurs catégories de fichiers ou de mails.

Elle ne peut être décidée que par l'autorité de direction compétente et non par l'administrateur du réseau.

Les résultats de cette surveillance sont portés à la connaissance de la seule autorité de direction l'ayant ordonné, qui prendra ou proposera les mesures nécessaires au regard du résultat communiqué (voir § 31)

Dans les deux types de surveillance, les personnels administrant le réseau sont conduits à prendre connaissance volontairement ou involontairement de données confidentielles notamment des informations qui relèvent de la vie privée des utilisateurs du réseau, ils sont donc astreints à une **stricte obligation de confidentialité** et ne doivent en aucun cas révéler à quiconque le contenu ou l'existence de ces informations sauf les cas prévus qui imposent de rendre compte à l'autorité de direction compétente.