Fiche pratique

L'utilisation de logiciels de contrôle d'ordinateur et de gestion de classe

Dans le cadre de leurs missions, les établissements scolaires peuvent avoir recours à des logiciels de contrôle et de gestion de classe (« le Logiciel COGC »). En effet, ce type de logiciel permet de garder un certain contrôle sur l'utilisation faite par les élèves des outils numériques (ordinateurs, tablettes, smartphones, etc…) Par exemple, le Logiciel COGC permet notamment de partager son écran, de prendre le contrôle sur un appareil ou encore de limiter l'accès au web.

Si le Logiciel COGC n'est pas illégal en lui-même, il est toutefois nécessaire d'en faire un usage réfléchi afin de préserver l'intimité et la vie privée des élèves.

L'objectif de cette fiche pratique est de fournir aux établissements scolaires des outils pour leur permettre de mieux appréhender la mise en balance à effectuer entre la nécessité pour les enseignants de contrôler l'usage des outils informatiques par les élèves et la protection de leur vie privée, ainsi que leur droit à ne pas être soumis à une surveillance permanente.

Cette fiche pratique ne remplace pas l'analyse[1] qui doit être faite par chaque établissement scolaire avant l'utilisation des logiciels de contrôle d'ordinateur.

Information

La première chose à faire lors du déploiement d'un Logiciel COGC est d'**informer**, non seulement les élèves mais également leurs représentants légaux. Il est important qu'ils connaissent avec un certain degré de précision l'étendue de la surveillance dont ils font l'objet.

Ainsi, une simple mention de l'utilisation d'un logiciel de contrôle et de gestion de classe sera insuffisante dans la majorité des cas. Des explications un peu plus fournies sur les usages surveillés et la temporalité de surveillance seront très souvent nécessaires. Par ailleurs, cette information doit être facilement accessible et compréhensible pour le public cible, c'est-à-dire, les élèves.

Aucune utilisation de ce type de logiciel ne pourra être considérée comme conforme sans cette information. Aussi, toutes les hypothèses évoquées ci-dessous impliquent une information adéquate préalable.

[1] L'analyse doit notamment être conduite au regard du principe de minimisation prévu à l'article 5 du RGPD. Si par ailleurs, le traitement est basé sur l'intérêt légitime, un exercice de mise en balance devra être effectué au regard de l'article 6.1.f du RGPD.

Fiche pratique

L'utilisation de logiciels de contrôle d'ordinateur et de gestion de classe

Conditions d'utilisation du logiciels de contrôle d'ordinateur et de gestion de classe

Scénario 1 : ordinateur fixe en salle de classe

Le Logiciel COCG est installé sur les ordinateurs fixes d'une seule classe (la salle informatique par exemple).

Dans ce scénario, l'utilisation du Logiciel COCG ne semble pas soulever de difficulté particulière. En effet, la surveillance des élèves est strictement limitée dans le temps (la durée du cours) et dans l'espace (uniquement la salle de classe concernée).

En revanche, si toutes les salles de classes sont équipées d'ordinateurs fixes et que tous les ordinateurs disposent d'un logiciel de surveillance sans restriction particulière, cela pourrait conduire à une surveillance permanente de fait.

Nous renvoyons dès lors aux points de vigilance du scénario numéro 2.

Scénario 2 : mise à disposition d'une tablette ou d'un ordinateur portable équipé d'un Logiciel COGC par l'établissement scolaire avec restitution en fin d'année ou de cycle.

La simple portabilité de l'outil soulève des questionnements importants : les élèves peuvent-ils utiliser l'outil à la maison ? Si oui, à quelles fins ? Sont-ils autorisés à utiliser l'outil pour leurs loisirs ? L'utilisation est-elle juste limitée à des finalités scolaires ?

Lorsque la surveillance envisagée n'a pas d'utilité avérée sur le plan éducatif et/ou risque de dépasser le cadre scolaire, il est fortement recommandé de ne pas la mettre en place.

Même lorsque la mise à disposition des outils s'accompagne de l'interdiction de les utiliser pour des finalités personnelles, il n'en reste pas moins que la portabilité de l'objet rend la surveillance des élèves permanente ou quasi permanente. Ils sont alors surveillés dans chaque cours, tous les jours, toutes les semaines y compris lorsqu'ils travaillent le soir à la maison ou pendant les vacances scolaires.

Pour qu'une telle surveillance puisse être considérée comme proportionnée, de sérieuses garanties devront être déployées, comme par exemple :

- S'assurer que l'activation de l'outil n'est pas possible en dehors des heures de cours habituelles ;
- Privilégier les fonctionnalités les moins intrusives (une limitation d'accès est moins intrusive qu'un enregistrement) ;
- S'assurer de la traçabilité de l'activation et de la désactivation (Qui ? Quand ?) du logiciel COGC

Pour rappel, ces garanties viennent s'ajouter aux mesures de transparence évoquées dans la partie « INFORMATION » de cette fiche pratique.

Fiche pratique

L'utilisation de logiciels de contrôle d'ordinateur et de gestion de classe

Scénario 3 : L'installation du logiciel de contrôle sur des outils appartenant aux élèves (BYOD).

La CNPD recommande de manière générale de ne pas installer des logiciels de contrôle sur des outils appartenant aux élèves et que ceux-ci seraient entre autres amenés à utiliser à l'école, car cela implique une lourde intrusion dans la vie des élèves qui dépasse le cadre scolaire.

Toutefois, si l'établissement scolaire offre une solution technique permettant de séparer les usages privés et scolaires sur le terminal de l'élève alors ce scénario pourrait être envisagé. A titre d'exemple, les solutions de type :

- Conteneurisation - le logiciel et les données seraient isolés dans un conteneur et donc séparé de l'environnement des autres applications - ou,
- Clonage du système d'exploitation - par exemple, celui d'origine serait dédié à l'utilisation privée et le clone à l'utilisation scolaire ;

pourraient éventuellement répondre à cette nécessité de séparation des deux usages. Quoi qu'il en soit, les limites et réserves mentionnées dans le scénario 2 trouvent à s'appliquer dans ce cas également en raison de la portabilité du terminal.

Par ailleurs, les établissements scolaires qui souhaiteraient explorer cette piste auront de nombreux défis à relever, en particulier en ce qui concerne la sécurité, car ils n'auront pas d'homogénéité technique sur les différents terminaux concernés, ni la maîtrise desdits terminaux (qui reste la propriété des élèves).

FOCUS : base légale

Tout traitement de données à caractère personnel doit reposer sur une base légale. Parmi les bases légales prévues par le RGPD[2], celle qui semble la plus appropriée est l'intérêt légitime. Il est donc recommandé de bien documenter l'exercice de mise en balance entre les intérêts légitimes poursuivis par l'établissement scolaire (considérations éducatives et/ou disciplinaires) et les droits fondamentaux des élèves (respect de leur intimité et vie privée).

Il pourrait être tentant de baser le traitement objet de la présente fiche sur le consentement. La plus grande prudence est de mise ici car un consentement ne peut en aucun cas être valide s'il n'est pas libre. Or, si l'élève est contraint de consentir pour pouvoir accéder à l'outil informatique, le consentement ne peut pas être valable.

Ajoutons à cela que les élèves sont pour la plupart mineurs, ce qui ajoute de la complexité au recueil et à la validité du consentement.

[2] Article 6 du RGPD : « Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant."

Cette fiche pratique n'est pas exhaustive quant aux différentes utilisations possibles de ces outils. Elle ne peut en aucun cas constituer un accord ou désaccord de principe ni préjuger sur le droit de la CNPD d'entreprendre des démarches et mesures à l'égard d'un responsable de traitement. Seule une analyse individuelle de chaque situation permettrait d'aboutir à une telle conclusion.

Par ailleurs, quel que soit le scénario envisagé, il sera nécessaire de s'assurer que la sécurité et la confidentialité des données et des terminaux (appareils fournis par l'établissement ou BYOD) sont conformes à l'état de l'art, en particulier en cas d'hébergement des données par un prestataire externe.