SNT INFO SYNDICAT NATIONAL DES TERRITORIAUX CFE CGC
Ensemble et pour tous

CE QU'ON NE VOUS DIT PAS EN MATIÉRE DE

LOGICIEL ESPION

Le contrôle sans modération des salariés est loin d'être une idée judicieuse. Il établit un rapport hiérarchique et installe la méfiance qui finalement démotive les salariés. Surveiller les salariés pour les contrôler n'est guère une méthode appréciée de management. Cette pratique à la limite du légal met à mal les valeurs que l'on voudrait ériger dans son entreprise. En France l'espionnage des salariés est condamné par la loi. Pourtant les vendeurs de logiciels espions font les yeux doux aux chefs d'entreprise ou aux administrations pour les attirer dans cette spirale.

QUE DIT LE DROIT ?

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) rappelle que l'intimité de la vie privée et le secret des communications électroniques sont protégés par la loi. Leur violation, la vente au public et l'utilisation de dispositifs d'écoute sont illégales et passibles de poursuites judiciaires.

Un chef d'entreprise ou une direction, a le droit d'effectuer un contrôle sur les salariés ou les agents, de vérifier qu'ils suivent les consignes qui leur sont données tant pour le développement de l'entreprise ou de la direction, que leur sécurité et celle de leurs collègues. Cependant, ce droit de contrôle se doit de respecter les droits des salariés ou des agents.

EST-CE QUE LE CHEF D'ENTREPRISE OU L'ADMINISTRATION PEUT CONTROLER L'UTILISATION D'INTERNET ?

Selon la CNIL, les conditions et les limites de l'utilisation d'internet peuvent être fixées par l'entreprise ou l'administration. Ces limites ne constituent pas, en soi, une atteinte à la vie privée des salariés (dispositifs de filtrage de sites non autorisés notamment pour les sites à caractère pornographique, pédophile, d'incitation à la haine raciale, révisionnistes, etc.), limites dictées par l'exigence de sécurité de l'organisme, telles que l'interdiction de télécharger des logiciels, de se connecter à un forum ou encore d'utiliser le « chat », l'interdiction d'accéder à une boîte aux lettres personnelle par internet compte tenu des risques de virus qu'un tel accès est susceptible de présenter, etc.

Il s'agit en réalité ici de protéger l'entreprise ou l'administration contre d'éventuelles intrusions notamment informatiques.

LES DIVERSES FORMES D'ESPIONNAGE ?

En revanche, l'espionnage et le fait de contrôler son salarié ou son agent à son insu est interdit par la loi :

- espionnage des mails, des ordinateurs, des téléphones,
- géolocalisation des salariés,
- écoutes téléphoniques…

Aujourd'hui c'est internet qui a la faveur de l'espionnage par les biais les plus divers. Les logiciels sont souvent gratuits et d'une utilisation qui ne présente aucune difficulté. Ils démarrent à chaque ouverture de session sans que l'utilisateur ne s'en aperçoive, et inscrit les clics effectués, les frappes sur le clavier, les pages internet visitées…

COMMENT DÉCLARER ?

La CNIL préconise les points suivants : il est interdit d'utiliser ces logiciels dans un cadre professionnel sauf en cas de forts impératifs de sécurité (lutte contre la divulgation de secrets industriels par exemple). Les salariés doivent être informés des dispositifs mis en place et des modalités de contrôle de l'utilisation d'internet : le comité social d'entreprise (ou le comité social territorial pour nous) doit avoir été consulté et informé (article L2323-32 du code du travail) ; les salariés doivent être informés, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées. Une durée de conservation de l'ordre de six mois est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet.

La charte informatique du Conseil départemental prévoit que la conservation des données ne peut excéder 12 mois :

> *« Section III.3 Mesures de contrôle de la sécurité :*
>
> *Le Conseil départemental des Vosges est dans l'obligation de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. Il s'appuie pour ce faire sur des fichiers de journalisation (fichiers logs) qui recensent toutes les connexions ou tentatives de connexions au système d'informations du Conseil départemental des Vosges. Ces fichiers comportent les données suivantes : dates, identifiants, objet de l'événement. Le service informatique du Conseil départemental des Vosges est le seul utilisateur de ces informations dont la conservation ne peut excéder 12 mois et qui sont effacées à l'issue de ce délai maximum. »*

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste, le traitement ainsi mis en œuvre doit être déclaré à la CNIL (déclaration normale) sauf si un correspondant informatique et libertés a été désigné, auquel cas aucune déclaration n'est nécessaire.

La collectivité semble vouloir acquérir un logiciel de ce type : « NEXTHINK »

Rappelons que chaque utilisateur de la collectivité a signé la charte informatique qui précise que :

> *« L'utilisateur est informé :*
>
> - *Que pour effectuer la maintenance corrective, curative ou évolutive, Le Conseil départemental des Vosges se réserve la possibilité de réaliser des*

interventions (le plus souvent à distance) sur les ressources matérielles et logicielles mises à sa disposition ;

- *Qu'une maintenance à distance du poste de travail est précédée d'une information de l'utilisateur sauf cas d'urgence mettant en péril le système d'informations ou son intégrité et nécessitant une mesure immédiate ;*
- *Que toute situation bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste voire à la suppression des éléments en cause.*
- *Que l'ensemble du système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire, de suivi fonctionnel, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable. A ce titre, l'utilisateur est informé que les services informatiques du Conseil départemental des Vosges disposent d'outils techniques pour procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place. »*

Nous ne savons pas si cette déclaration obligatoire à la CNIL sera réalisée dans l'éventualité où la collectivité utiliserait ce logiciel.

LE CONTROLE DE L'UTILISATION DE LA MESSAGERIE ?

Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises ou les collectivités à mettre en place des outils de contrôle de la messagerie. Il est possible de contrôler le travail d'un salarié mais plusieurs règles doivent être respectées. **Lors de l'installation de tout dispositif de surveillance, le salarié et les institutions représentatives du personnel doivent en être informés.** L'utilisation doit évidemment être justifiée et le principe de proportionnalité respecté. A noter que certains dispositifs doivent également être déclarés à la CNIL.

L'employeur doit respecter le secret des correspondances privées. Une communication électronique émise ou reçue par un employé peut avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles L.226-15 (pour le secteur privé) et L.432-9 (pour le secteur public) du Code pénal.

« Extrait de la Charte informatique CD88 :

Contenu des messages électroniques :
Tout message adressé ou reçu par le biais de la messagerie mise à disposition de l'utilisateur par le Conseil départemental des Vosges est réputé dédié aux usages professionnels au sein du Conseil départemental des Vosges, sauf s'il comporte une

mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données. Pour préserver le bon fonctionnement des services, des limitations pourront être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus, …) seront déployées. »

DES LOGICIELS EXTREMEMENT INTRUSIFS DONT IL EST DIFFICILE DE GARDER LE CONTROLE

L'espionnage à mauvais escient se retourne en général contre l'entreprise ou la direction car il détruit la confiance. Les salariés sont très attentifs au respect de leur vie privée mais aussi professionnelle et le risque encouru est de perdre sa notoriété et donc de faire fuir les talents.

Protéger son entreprise ou sa collectivité ainsi que ses salariés, oui.

Les espionner, non.

Nous demanderons donc à la direction lors d'un prochain dialogue social la réalité des faits concernant l'acquisition de ce logiciel et aussi les modalités de mise en place de celui-ci et l'impact qu'il pourrait avoir sur les agents.