

Focus sur la messagerie professionnelle au travail

La messagerie professionnelle est aujourd'hui devenue un outil indispensable et bien souvent nécessaire à l'accomplissement, par l'employé, de ses missions de travail. Toutefois, la banalisation d'un tel dispositif de communication électronique n'exonère pas pour autant l'employeur du respect des dispositions relatives à la protection des informations nominatives, et bien qu'il puisse décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie mise à disposition de ses salariés, notamment pour des raisons de sécurité, il est tenu également par l'obligation de respecter la vie privée de ces derniers.

En Principauté, en effet, conformément à l'article 22 de la Constitution, « *Toute personne a droit au respect de sa vie privée et familiale et au secret de sa correspondance* ».

De même, dans un arrêt *Niemietz c. Allemagne* en date du 16 décembre 1992, la Cour Européenne des Droits de l'Homme (CEDH) a consacré le droit au respect de la vie privée sur le lieu de travail en se fondant sur l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, aux termes duquel « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

Quelques années plus tard, cette même Cour a précisé les conditions dans lesquelles l'employeur peut consulter les communications numériques de son salarié dans son arrêt *Bărbulescu c. Roumanie* en date de 2017.

En l'espèce, un salarié qui avait communiqué avec sa famille à partir de son poste de travail, sur un compte de messagerie destiné à un usage professionnel, avait été licencié, au motif qu'il n'avait pas respecté le règlement intérieur qui interdisait l'utilisation des ressources de l'entreprise à des fins personnelles.

La Cour a toutefois estimé que ce licenciement était contraire au droit à la protection de la vie privée, consacré à l'article 8 de la Convention européenne des droits de l'homme puisque si l'employeur est en droit de surveiller les communications électroniques de son salarié, l'étendue de la surveillance et le degré d'intrusion dans la vie privée du salarié ne doivent pas être disproportionnés par rapport au but recherché. Par ailleurs, il incombe aux juges de vérifier que l'accès au contenu des communications n'a été mis en place que parce qu'il n'existait pas de mesures moins intrusives, et de s'assurer que les conséquences de la surveillance pour le salarié ne sont pas disproportionnées par rapport au but recherché.

Pour tout responsable de traitement, entrent ainsi en conflit deux intérêts apparemment contradictoires, mais néanmoins conciliables, à savoir d'un côté le droit au respect de la vie privée et au secret des correspondance des employés et d'un autre le respect des intérêts légitimes de l'employeur, entre lesquels il convient de trouver un juste équilibre.

Cette fiche pratique a donc vocation à résumer les droits et obligations des employeurs vis-à-vis de leurs employés s'agissant de l'utilisation de la messagerie électronique professionnelle.

➤ **Principe de la protection des correspondances privées sur le lieu de travail**

Pour la Commission, le respect du secret des correspondances privées est un principe intangible. Ainsi, l'employeur ne peut accéder aux contenus des messages privés de ses employés envoyés ou reçus à partir de la messagerie professionnelle, sans que ledit employé soit présent, et en soit expressément d'accord.

Toutefois, pour que les messages soient considérés comme personnels, il convient pour les employés de les identifier comme tels, par exemple :

- en précisant dans l'objet du message des mots clés comme « **privé** », « **[PRV]** » ou encore « **personnel** » ;
- en incluant dans l'objet du message une mention laissant manifestement supposer que ledit message est privé, telle que « *vacances au Japon* » ;
- en stockant les messages dans un répertoire intitulé « *personnel* » ou « *privé* ».

La Commission considère donc comme excessive la pratique consistant pour l'employeur à recevoir tous les messages envoyés ou reçus par ses employés puisque cette pratique ne permet pas de distinguer entre les messages professionnels et personnels desdits employés.

Par ailleurs, seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi. Cela peut notamment prendre la forme d'une Ordonnance judiciaire mandatant un huissier de justice aux fins d'accéder, voire d'enregistrer les messages privés litigieux.

➤ **Fonctionnalités autorisées**

La Commission estime que tout traitement automatisé de messagerie professionnelle peut notamment avoir les fonctionnalités suivantes :

- l'échange de messages électroniques en interne ou avec l'extérieur ;
- l'historisation des messages électroniques entrants et sortants ;
- la gestion des contacts de la messagerie électronique ;
- la gestion des dossiers de la messagerie et des messages archivés ;
- l'établissement et lecture de fichiers journaux ;
- la gestion des habilitations d'accès à la messagerie ;
- la gestion de l'agenda ;
- l'établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).

Par ailleurs, lorsqu'une surveillance est mise en œuvre sur le lieu de travail, la messagerie professionnelle peut également avoir également pour fonctionnalité(s) :

- la mise en place d'une procédure de contrôle gradué ;
- le contrôle au moyen d'un logiciel d'analyse des messages électroniques entrants ou sortants.

Quid de la notion de surveillance ou de contrôle

Un employeur peut décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie professionnelle mise à la disposition de ses employés. A cet égard, la Commission indique que cette notion de contrôle ou de surveillance de la messagerie électronique se conçoit comme « *toute activité qui, opérée au moyen d'un logiciel d'analyse du contenu des messages électroniques entrants et/ou sortants, consiste en l'observation, la collecte ou l'enregistrement, de manière non occasionnelle, des données à caractère personnel d'une ou de plusieurs personnes, relatives à des mouvements, des communications ou à l'utilisation de la messagerie électronique* ».

➤ **Dispositions à prendre en cas d'absence de l'employé**

Afin d'assurer la continuité des affaires de l'entreprise pendant l'absence d'un salarié (congés, maladie...), la Commission estime que l'employeur pourra avoir accès aux messages professionnels dudit salarié, en utilisant une des méthodes suivantes :

- mise en place d'une réponse automatique d'absence du bureau à l'expéditeur avec indication des personnes à contacter en cas d'urgence ;
- désignation d'un suppléant qui dispose d'un droit d'accès personnalisé à la messagerie de son collègue ;
- transfert à un suppléant de tous les messages entrants.

Dans les deux derniers cas, le salarié devra toutefois être informé de l'identité de son suppléant et ce suppléant ne devra pas lire les messages identifiés comme privés ou personnels.

➤ **Modalités d'information des utilisateurs**

Tout employeur doit impérativement responsabiliser les utilisateurs à la protection de leurs informations nominatives. Dans un souci de transparence envers les utilisateurs, ainsi que de loyauté dans la collecte et le traitement des informations nominatives, la Commission recommande donc à l'employeur de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les modalités d'identification des messages privés ;
- la procédure d'accès à la messagerie par des personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur, et ce afin d'assurer la continuité des activités.

➤ **Modalités d'information des tiers destinataires**

La Commission recommande l'insertion d'une mention d'information au bas de tout message électronique sortant, afin d'informer les tiers destinataires de la finalité du traitement, ainsi que de leurs droits.

Exemple de message

Vos informations nominatives sont exploitées par [Nom de l'employeur] dans le cadre du traitement ayant pour finalité "[Finalité du traitement]". Conformément à la Loi n° 1.165 du 23 décembre 1993, vous disposez d'un droit d'accès, de rectification et de suppression en écrivant [adresse de l'employeur].

➤ **Données collectées**

La Commission considère que les catégories suivantes de données peuvent être collectées et traitées :

- Données communes à l'ensemble des messageries :
 - identité : nom, prénom, identifiant ;
 - messages : date, heure, information expéditeurs/destinataires, contenu, objet ;
 - gestion des contacts : nom, prénom, raison sociale, (...) ;
 - données d'identification électronique : adresse de messagerie électronique ;
 - journalisation des accès : logs de connexion des personnels habilités à avoir accès au traitement ;
 - fichiers journaux : date et heure du message, nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages, (...) ;
 - habilitations : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés ;

- Données particulières aux messageries mises en œuvre à des fins de surveillance ou de contrôle :
 - gestion des alertes : réception des alertes automatiques en fonction des niveaux hiérarchiques concernés.

- **Durées de conservation des données**

La Commission rappelle que conformément à l'article 10-1 de la Loi n° 1.165, modifiée, les informations nominatives ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont exploitées.

Ainsi, au regard des fonctionnalités de la messagerie, la Commission demande au responsable de traitement de prévoir les durées de conservation de données suivantes :

- s'agissant de l'administration de la messagerie électronique (identité, gestion des contacts, données d'identification électronique) : 3 mois **maximum** après le départ définitif de l'utilisateur.

A cet égard, la Commission rappelle que lors du départ définitif de l'utilisateur, sa boîte email nominative doit être immédiatement « **bloquée** » c'est à dire qu'elle ne doit plus pouvoir recevoir d'emails, ni en envoyer, à l'exception d'un message automatique qui sera adressé à chaque personne ayant envoyé un email à l'adresse concernée.

Ce message automatique a vocation à informer l'expéditeur de l'email que son interlocuteur ne travaille plus au sein de l'entité, et qu'il devra désormais envoyer ses emails à telle ou telle adresse. Ceci pourra être pratiqué pendant 3 mois au maximum, selon les fonctions et le degré de responsabilité de l'ancien salarié.

A l'échéance de cette période de trois mois maximum, l'adresse email nominative de l'ancien salarié sera désactivée (supprimée).

L'employeur doit avertir l'employé de la date de fermeture de son compte et lui permettre de récupérer les emails privés susceptibles de se trouver dans sa boîte email nominative professionnelle.

- s'agissant du contenu des messages émis et reçus : entre 2 et 3 ans maximum dans la boîte active de l'utilisateur puis ensuite, si besoin, mettre en place une **politique d'archivage**.

La Commission reconnaît en effet que les messages électroniques des collaborateurs peuvent être conservés durant plusieurs années notamment en ce qui concerne les établissements bancaires et assimilés à des fins de traçabilité des opérations financières, ou en cas de soupçons d'activités illicites.

Les messages récents peuvent être stockés dans la messagerie interne du collaborateur pendant une période n'excédant pas 3 ans maximum (archives courantes) puis être automatiquement effacés de sa messagerie, afin d'être conservés dans un serveur distinct jusqu'à l'expiration du délai nécessaire (archives intermédiaires) avec des accès restreints aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, le service du contentieux).

- s'agissant de la journalisation des accès et des fichiers journaux : de 3 mois à 1 an maximum, en fonction de l'activité exercée.
- s'agissant des alertes : la Commission demande que les données relatives à un événement ne mettant pas en lumière un incident (faux positifs par exemple) soient immédiatement supprimées après analyse.

En cas d'incident avéré les données doivent être conservées le temps nécessaire à la réalisation de l'enquête associée, conformément à la législation applicable.

- s'agissant des habilitations : le temps de l'affectation.

En tout état de cause, la Commission recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les données traitées ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées.

Enfin, la Commission rappelle que dans le cadre de l'ouverture d'une procédure contentieuse, toute information nécessaire issue du traitement pourra être conservée jusqu'à la fin de ladite procédure.

- ***Mesures de sécurité à mettre en place***

La Commission rappelle que les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du traitement.

Les mots de passe doivent être forts et régulièrement renouvelés.

Les accès à distance à la messagerie doivent être sécurisés.

L'employeur doit régulièrement sensibiliser les utilisateurs à la sécurité de leur messagerie (par exemple : ne jamais ouvrir les pièces jointes provenant d'un expéditeur inconnu, ne pas cliquer sur des hyperliens dans les emails, ne pas envoyer de données sensibles ou importantes par email non sécurisé).