Recommandations

I. Nous formulons ci-après plusieurs règles de conduite juridiques autour de quatre thèmes qui constituent des exemples ou des outils permettant de tenir compte de la LVP lors d'un accès patronal à des communications électroniques ou d'un contrôle de ces dernières.

Commençons toutefois par une recommandation de base.

À titre de recommandation générale de base, il convient d'élaborer au maximum des règles préventives (sur le plan juridique, en lien avec le management et sur le plan technique) ainsi que des procédures préventives (par exemple pour le classement d'e-mails, de documents, de fichiers) afin d'éviter que survienne le besoin dans le chef de l'employeur de contrôler et d'accéder à des informations personnelles des travailleurs.

En la matière, si l'employeur a un rôle à jouer, c'est également le cas des personnes concernées elles-mêmes. Les membres du personnel sont tenus à un devoir de rigueur en ce qui concerne leurs propres données à caractère personnel disponibles sur le lieu de travail (par exemple, des données relatives à des évaluations, des fiches de salaire, …) et doivent dès lors les protéger suffisamment à l'égard de tiers, et ce même au sein de l'entreprise ou de l'administration publique.

Cela vaut par exemple aussi pour des e-mails privés reçus ou envoyés sur le lieu de travail. Les travailleurs utilisent en effet aussi le système d'e-mails de l'employeur à des fins privées, dans une plus ou moins grande mesure, surtout si cela a été explicitement autorisé par l'employeur.

Les travailleurs ont certes le droit d'effectuer des communications privées sur le lieu de travail, dans une mesure limitée, mais pour protéger leur vie privée, mieux vaut séparer autant que possible les e-mails professionnels des e-mails privés.

Les e-mails privés reçus ou envoyés pendant les heures de travail par le travailleur ne sont en effet *a priori* pas destinés à être lus ou reçus par l'employeur, et certainement pas en ce qui concerne leur contenu[1].

Les e-mails fonctionnels doivent par contre *a priori* pouvoir être traités dans le contexte normal de communication professionnelle au sein d'une entreprise/administration publique – et il en va de même en ce qui concerne leur contenu -, étant donné qu'ils concernent évidemment l'exécution de la tâche de travail au sens strict.

En cas de double utilisation du système d'e-mails, il est toutefois difficile de concilier les droits et intérêts des deux parties.

[1] Toutefois, du fait qu'ils sont générés pendant les heures de service, l'employeur doit pouvoir suivre l'existence de certaines communications privées de ses subalternes étant donné qu'elles peuvent compromettre la bonne exécution de la tâche de travail (abus des heures de travail), mais un accès direct au contenu reviendrait à une individualisation du contenu des messages, ce qui est contraire à la CCT n° 81.

Dans ce cas, bien que l'intention de l'employeur se limite à la prise de connaissance du contenu des e-mails à caractère professionnel en vue de la gestion et de l'organisation de ses activités (et non en vue de "contrôler" un quelconque abus du système d'e-mails), cet employeur portera quoi qu'il en soit atteinte à la vie privée de l'utilisateur final.

En effet, il sera inévitablement confronté à des e-mails non professionnels, alors que la prise de connaissance de l'existence de tels e-mails (sans parler de leur contenu) ne serait en fait possible qu'à la suite de l'approche graduelle de la CCT n° 81 (d'abord, un contrôle anonyme et ensuite, un contrôle individualisé) et moyennant le respect des règles d'individualisation prévues par cette CCT.

Dans un tel contexte, une solution est évidente : elle consiste à éviter la double utilisation du système d'e-mails de l'employeur. Le problème de l'accès direct aux e-mails privés des travailleurs ne se pose ainsi normalement plus.

Cette méthode peut être appliquée en demandant aux travailleurs d'utiliser une adresse e-mail personnelle (de type Hotmail) pour leurs e-mails privés, et non l'adresse e-mail mise à sa disposition pour pouvoir exécuter les activités professionnelles.

Si l'employeur a précisé dans sa politique ICT que le double usage de son système d'e-mails (professionnel et privé) est interdit, il peut en principe considérer que les e-mails ont un caractère professionnel, surtout en ce qui concerne les messages envoyés[2].

Un éventuel accès direct à de tels e-mails d'un travailleur peut dès lors se justifier, moyennant le respect des grands principes de base de la LVP, à savoir un accès limité à des finalités déterminées, explicites et légitimes ; cet accès doit en outre être adéquat, pertinent et non excessif au regard des finalités et à condition d'avoir fourni des informations adéquates quant à cet accès.

Si l'employeur tombe néanmoins sur un e-mail privé lors d'un tel accès direct, il en prend connaissance de manière légitime. Cela ne signifie pas pour autant qu'un e-mail privé dont l'employeur prend ainsi connaissance puisse ensuite être utilisé pour un but quelconque (par exemple, une utilisation dans une intention frauduleuse ou en vue de nuire au travailleur en question ou à un tiers). Une utilisation ultérieure de cet e-mail devra par contre respecter les exigences de la LVP.

Lorsque les employeurs ne peuvent ou ne veulent pas abandonner la double utilisation de leur système d'e-mails, ils devront inévitablement accepter qu'un membre du personnel puisse faire valoir des attentes supérieures en matière de vie privée à l'égard de sa boîte aux lettres électronique. On peut en effet difficilement défendre une interdiction absolue d'utiliser le système d'e-mails de l'employeur à des fins privées, même de manière limitée.

Une telle boîte aux lettres mixte ne peut dès lors pas être consultable directement et intégralement par l'employeur. Il faudra par contre convenir d'une procédure complémentaire pour faire la distinction entre les deux types de messages, par exemple en demandant au travailleur de classer les e-mails reçus et envoyés. La prise de connaissance patronale de l'existence d'e-mails classés comme étant privés (sans parler de leur contenu) ne serait alors en fait possible qu'à la suite de l'approche

[2] En ce qui concerne les e-mails entrants, l'employeur devra être plus prudent qu'à l'égard des e-mails sortants, étant donné que l'employé n'en est pas l'auteur et n'attendait évidemment même pas certains d'entre eux.

graduelle de la CCT n° 81 et moyennant le respect des règles d'individualisation prévues par cette CCT.

Les recommandations suivantes s'appliquent dès lors surtout, mais pas exclusivement, aux employeurs qui permettent ou tolèrent la double utilisation de leur système d'e-mails.

Assurez-vous du respect du principe de légitimité, de la prévisibilité des traitements et de l'ingérence dans le droit au respect de la vie privée des travailleurs

- ne traitez des données à caractère personnel que dans les cas autorisés par la LVP ;

- prévoyez une participation et une consultation de la représentation des travailleurs ;

- informez les travailleurs des règles et conditions à respecter pour le contrôle ;

- définissez dans un document écrit la politique d'accès aux (données de) communications électroniques des travailleurs, de préférence dans le règlement de travail.

Limitez les possibles ingérences dans la vie privée des travailleurs

- limitez les possibilités de traitements d'un employeur en ce qui concerne des informations enregistrées sur les terminaux des utilisateurs finaux (par exemple, dans une boîte aux lettres professionnelle "mixte") à ce dont il a réellement besoin ;

- réalisez le traitement de données le moins intrusif (qui offre donc le moins de possibilités d'identification des personnes concernées par le traitement d'informations les plus générales possibles) ;

- motivez toute intrusion plus conséquente dans les données à caractère personnel des travailleurs, ou d'un travailleur en particulier, par des éléments de fait ;

- responsabilisez les travailleurs pour qu'ils se conforment aux règles relatives à l'utilisation d'Internet et de la messagerie électronique au travail, par exemple en activant la fonction "gestionnaire d'absence du bureau" de la messagerie (en mentionnant les personnes à contacter) de façon à ce qu'en cas d'absence, aucune intrusion dans leur support d'informations professionnel ne soit nécessaire ;

- prenez des mesures de prévention (techniques) pour éviter les abus par les travailleurs ;

- si la prévention ne suffit pas, ne contrôlez les abus qu'au moyen de la présence d'un certain flux de messagerie ou d'un comportement déterminé sur Internet, et ce selon le plan graduel prévu par la CCT n° 81 ;

- si la présence d'un certain flux de messagerie ou d'un comportement déterminé sur Internet ne suffit pas à constater l'abus, ne procédez à un contrôle que de manière exceptionnelle, par la prise de connaissance du contenu de la communication à laquelle le travailleur a participé.

Encadrez les opérations de surveillance et de contrôle

- à l'occasion d'un accès à des (données de) communications électroniques, que ce soit dans le cadre d'un contrôle ou non, ne traitez que des données à caractère personnel adéquates, pertinentes, précises et actualisées. Ces données ne peuvent pas être conservées pour une durée supérieure à celle nécessaire à la réalisation de la finalité ;

- veillez à ce que la personne chargée de la recherche et de la collecte de données à caractère personnel soit une autre personne que celle qui en donne l'ordre ;

- veillez à ce que la personne chargée de la recherche agisse sur la base d'instructions les plus précises possibles, formulées par le demandeur, et qu'elle se limite, dans sa recherche, à ce qui lui a été demandé ;

- veillez à ce que la recherche se fasse autant que possible sur la base de critères pertinents qui permettent dans un premier temps d'exclure de la consultation un maximum d'informations ;

- veillez à ce que la recherche ait lieu avant tout sur la base de dates, de mots clés, de l'identité des destinataires ou des expéditeurs de messages avant l'accès à leur contenu ;

- édictez des règles spécifiques en matière d'accès et d'utilisation pour le gestionnaire du système dans le cadre de l'exercice de sa fonction ;

- veillez à ce que les données à caractère personnel recherchées et recueillies légitimement grâce à l'accès continuent à bénéficier du degré de protection qui était le leur, du fait de leur statut légal (dans le cas par exemple d'un dossier du personnel, la personne chargée de procéder à l'accès sur demande de l'employeur est tenue, après cet accès, à la même confidentialité que le collaborateur qui gère normalement le dossier du personnel) ou par le statut qui leur a été donné, à titre professionnel, par le travailleur titulaire de l'outil ou par un éventuel correspondant (par exemple, une négociation encore confidentielle avec un tiers doit donc également rester tout aussi confidentielle après l'accès) ;

- ne prenez pas de décision importante à l'encontre de la personne concernée simplement sur la base d'informations collectées dans le cadre d'un traitement de ses données à caractère personnel (par exemple dans le cadre d'une opération de surveillance ou de contrôle) ;

- avant de prendre une quelconque décision à l'encontre de la personne concernée, offrez-lui la possibilité de faire valoir son point de vue, notamment quant à l'exactitude et à la pertinence des données à caractère personnel collectées.

Garantissez le respect des règles et renforcez la sécurité de la surveillance et du contrôle

- conservez un relevé écrit de l'ensemble des opérations constituant une intrusion dans les outils informatiques ou dans les informations qu'ils génèrent (ce qui a été consulté, collecté et transmis, quand, comment, pour le compte de qui, et par qui et à qui ces informations ont été communiquées) pour permettre tout contrôle du respect, par l'employeur, du principe de finalité et du principe de proportionnalité ;

-si la gestion et la maintenance des outils et des réseaux est réalisée par un prestataire externe, veillez à ce que les règles internes d'entreprise s'appliquent également à ce prestataire et concluez un contrat de sous-traitance avec un tel prestataire ;

- soumettez l'organisation des procédures mais aussi les opérations de surveillance et de contrôle concrètement envisagées, et de manière plus générale tous les accès aux outils informatiques, si disponibles, au préposé à la protection des données de l'entreprise afin qu'il puisse en apprécier le caractère nécessaire et licite ;

- prévoyez enfin une formation en protection des données destinée à responsabiliser les personnes contrôlées et permettant de générer de bonnes pratiques dans le chef du personnel chargé de la surveillance.

II. Nous formulons ci-après plusieurs règles de conduite pratiques qui constituent des exemples ou des outils permettant de tenir compte de la LVP lors d'un accès patronal à des communications électroniques ou d'un contrôle de ces dernières concernant les problèmes rencontrés le plus fréquemment. Toutefois, les solutions suggérées ne pourront jamais être transposées aveuglément, il appartient à chaque entreprise d'en évaluer la pertinence et de rechercher s'il n'existe pas d'autres solutions plus appropriées.

Certaines des pratiques citées relèvent plus de "trucs et ficelles" mais sont souvent des solutions efficaces pour résoudre des difficultés de respect des principes de protection de la vie privée.

Pratique n°1 : Séparer le privé du professionnel

Selon la recommandation de base, il convient d'indiquer quelles informations sont strictement privées.

Des entreprises ont convenu de ces indications selon les exemples ci-après. Ces pratiques permettent d'adapter les filtres de contrôle aux situations, notamment par la copie systématique du courrier professionnel envoyé, ce qui se juste pleinement dans le cas d'un contrôle interne d'ordres financiers donnés par courrier électronique.

1. Pour les informations, fichiers et documents

Exemple 1 : Stockage des informations privées

- Création sur le poste de travail d'un répertoire nommé "Privé-Nomdel'utilisateur" servant à stocker tous les documents non professionnels, répertoire ne pouvant contenir des informations professionnelles.

- Le répertoire privé est placé sur une partition du disque dur ne faisant pas l'objet de copies de sécurité (backup) centralisées et systématiques.

Exemple 2 : Stockage des informations professionnelles

- Les informations professionnelles, à l'exclusion de toute information privée, sont obligatoirement stockées sur le disque d'un serveur central, le cas échéant dans des répertoires réservés à l'utilisateur. Les documents professionnels sur le poste de travail n'étant que des copies, à considérer comme temporaire et ne faisant pas nécessairement l'objet de copies de sécurité systématique (celles-ci se faisant centralement pour les informations du serveur).

2. Pour les messages électroniques

Exemple 3 : Stockage des informations privées

- Création dans la boite de messagerie répertoire nommé "Privé-Nomdel'utilisateur" servant à stocker tous les messages non professionnels (envoyés et reçus), répertoire ne pouvant contenir des messages professionnels (les cas de non-respect pouvant faire l'objet de sanctions).

Exemple 4 : Utilisation de comptes distincts

- Attribution de deux (ou plus) comptes de messagerie avec des identifiants distincts pour chaque utilisateur, l'un pour la messagerie privée, les autres pour la messagerie professionnelle selon le type d'activité. Cette distinction se faire par le nom (exemple : initiales@domaine.com pour le professionnel et nom.prénom@domaine.com pour le privé) ou par le nom de domaine (exemple : nom@domaine.com pour le professionnel et nom@domaine.net pour le privé)

3. Pour les communications Internet

Exemple 5 : Utilisation de comptes distincts

- Attribution de deux (ou plus) identifiants d'utilisateurs selon le type d'activité. Une structure sémantique de l'identifiant permettant de nuancer les filtres de contrôle (nom0 pour le privé, nom, nom1, nom2, …pour le professionnel).

4. Par le distinction de postes de travail

Certains services ou segments de réseaux peuvent présenter une sensibilité particulière (ex. : locaux d'administration des systèmes et réseaux, service des ressources humaines, …). Dans ces cas il peut être légitime d'interdire toute activité privée sur ces postes de travail pour pouvoir les surveiller de manière stricte et permanente, tout en mettant à disposition d'autres postes de travail à disposition pour les activités moins sensibles ou privées. Une telle distinction peut aussi contribuer à l'efficacité des techniques de ségrégation des réseaux, comme les VLAN et les VPN.

5. Par le distinction dans la signature

Les signatures structurées dans les messages peuvent aussi constituer un critère distinctif entre le professionnel et le privé.

Exemple 6 : Utilisation de signatures distinctes avec une déclaration standard

- L'insertion automatisée de clauses d'avertissements standards pour accompagner les messages électroniques expédiés via le serveur ou une adresse de l'entreprise : soit une déclaration (« disclaimer ») précisant que le message est envoyé à titre privé et n'engage pas l'entreprise ; soit un avertissement concernant le caractère professionnel de la communication et la possibilité que le contenu de celle-ci fasse l'objet, sans justification nécessaire, d'une consultation ou d'une prise de connaissance par les responsables de l'entreprise.

<u>Pratique n°2 : Exclure des activités certaines opérations dangereuses</u>

Pour garantir le respect de certaines instructions d'utilisation des outils informatiques et éviter une surveillance qui donnerait accès à des informations sans utilité pour l'employeur, il peut être opportun d'empêcher certaines opérations via les outils de l'entreprise (par exemple, bloquer l'accès à certains sites ou de bloquer certaines adresses électroniques reconnues comme dangereuses) ou de programmer des messages d'alerte réservés à l'utilisateur en cas d'opérations suspectes. Les différentes fonctions et listes de sites et d'adresses d'expéditeurs à interdire sont proposées dans les logiciels spécifiques (suites de sécurité Internet) et peuvent être complétées par les besoins spécifiques de l'entreprise.

Si on compare les coûts et l'efficacité des protections des anti-virus avec celles des suites de sécurité Internet, on peut considérer la protection anti-virus comme insuffisante face aux menaces permanentes présentées par les réseaux Internet.

Pratique n°3 : L'accès aux communications personnelles exige un encadrement spécifique

Certaines communications professionnelles peuvent avoir un caractère spécifiquement personnel (par exemple par une mention dans l'objet). L'accès au contenu de ces communications, mêmes si elles sont clairement professionnelles, ne pourra se faire qu'avec la prudence appropriée.

Exemple 1 :

- Indication "PERSONNEL" ou "CONFIDENTIEL" dans l'objet du message. Toutefois, il semble difficile d'obtenir cette discipline pour les tiers envoyant des messages à l'entreprise.

Exemple 2 :

- Utilisation de répertoires spécifiques, au sein des espaces réservés aux informations professionnelles

Exemple 3 :

- Pour sélectionner les messages et leur donner la fin nécessaire, on désignera une personne de confiance, neutre, soumise au devoir de confidentialité et habilitée à apprécier la qualité du message. Ce n'est qu'exceptionnellement qu'un supérieur hiérarchique, un collègue ou un assistant administratif sera la personne appropriée.

Exemple 4 :

- Lorsque des informations ont un caractère sensible les reporter dans des pièces attachées qui peuvent être protégées de manière spécifique.

Exemple 5 :

- Lorsque des personnes traitent couramment des informations d'une catégorie confidentielle (exemples : données médicales, délibéré d'un jury) ne permettre l'accès pour contrôle qu'à des personnes habilitées à accéder à cette catégorie de données (exemple : un médecin pour les données médicales).

Pratique n°4 : Limiter la surveillance aux données nécessaires et non réutilisation des données collectées

Dans la mesure où l'intrusion dans l'outil de travail informatique ou de communication électronique permet facilement de collecter d'autres informations que celles (adéquates, pertinentes et non-excessives) concernées par la finalité de l'opération de surveillance, l'accès aux données, leur recherche, leur collecte et leur transmission devraient être encadrés par des procédures de limitation.

Exemples :

- Extraction, en temps réel ou dès que possible, des données de surveillance journaux, logs, traces) pour un stockage dans une zone sécurisée ("silo" : serveur spécifique, fichier chiffré, …) dont les accès sont strictement limités et tracés spécifiquement.

- Précision, dans la politique de sécurité de l'information, de l'interdiction d'utiliser les informations de surveillance à toutes autres fins que celles définies dans le cadre de la surveillance.

Pratique n°5 : Instaurer des incompatibilités dans les droits d'accès pour une même personne

Un utilisateur ne devrait pas pouvoir dissimuler ses actions illicites, par exemple en pouvant modifier les traces générées par ses actions. De telles limitations sont aujourd'hui possibles par le biais des outils de gestion des identités et des accès.

Pratique n°6 : Gestion des traces

Les procédures de prises de traces, de leur manipulation, de leur sauvegarde et leur protection doivent être explicites et suffisamment précises pour créer la confiance suffisante pour une reconnaissance de recevabilité et d'opposabilité par les parties. La Commission n'a pas à préconiser une quelconque technique mais suggère quelques exemples de possibilités :

Exemples :

- Création d'un fichier cumul des traces, avant toute analyse, de manière séquentielle et incrémentale rendant toute altération ultérieure difficile si pas impossible.

- Calcul d'une empreinte avant toute analyse et sauvegardée de manière sécurisée.

- Auditabilité du respect pratique et quotidien de la bonne mise en pratique des procédures

- En cours de traitements tracés, verrouillage permettant d'empêcher la désactivation des traces ou leur modification.

- Scellement des traces en temps réel assurant l'authenticité et l'intégrité, par l'utilisation d'outils cryptographiques appropriés.

Pratique n°7 : Définir les règles de fonctionnement dans les cas d'exceptions

L'utilisation normale de l'outil informatique permet d'assurer la surveillance par des règles relativement simples. Toutefois, de multiples situations d'exceptions occasionnent de sérieuses difficultés lorsqu'elles n'ont pas été prévues et cadrées par des règles appropriées.

1. Absence planifiée d'un travailleur

Exemples de pratiques:

- Réponse automatique à l'expéditeur le prévenant de l'absence et lui donnant les indications pour transmettre le message à une personne appropriée si le message ne peut attendre le retour de la personne (principe des messages "Out of Office")

- La personne convient d'une personne de confiance habilitée à sélecter les messages ou les fichiers professionnels en cas de nécessité justifiée et d'une urgence ne pouvant attendre le retour.

2. Absence non planifiée ou fortuite d'un travailleur

La procédure prévue dans le cadre de la politique de sécurité de l'information ou du règlement de travail devra prévoir les modalités et les critères de choix de la personne de confiance habilitée à accéder aux informations du travailleur.

Exemples :

- Une personne désignée préalablement et reconnue comme "sage", habilitée à traiter les cas délicats (exemple en milieu hospitalier : le médiateur hospitalier)

- Une personne désignée de cas en cas, par accord entre l'employeur et un représentant du personnel.

3. Démission ou licenciement du travailleur avec ou sans prestation du préavis

Les situations de démission ou de licenciement (pour faute grave ou non) sont toujours délicates et sources de difficultés. La procédure sera analogue à celle à prévoir pour l'absence non planifiée. De plus, la procédure devra préciser la bonne fin à donner aux messages destinés au travailleur licencié et aux fichiers professionnels et privés stockés sur le poste de travail.

Exemples de pratiques:

- En cas de départ avec prestation du préavis, prévoir une procédure analogue à celle prévue pour les absences planifiées du travailleur, le cas échéant en concertation avec le travailleur au moment du départ.

- En cas de départ sans prestation du préavis, une personne est désignée de cas en cas, par accord entre l'employeur et un représentant du personnel ; cette personne étant habilitée à gérer les messages arrivant au nom du travailleur.

- Prévoir dans la politique de sécurité la suite à donner aux messages professionnels (transfert à un autre travailleur approprié) et aux messages privés (effacement ou transfert ou vers une adresse privée pendant une durée limitée de 1 mois). Il n'est pas toujours recommandé d'indiquer dans le message automatique de réponse à l'expéditeur que le travailleur ne fait plus partie du personnel de l'organisme ; une telle indication ne pourra donc se faire qu'avec le consentement explicite et formel du travailleur.

- Prévoir dans la politique de sécurité la suite à donner aux fichiers et informations à caractère privé (les fichiers et informations professionnelles pouvant être utilisés par l'employeur selon les règles internes).

4. Suspicion de fraude ou d'une malveillance dans le chef du travailleur

Les situations de démission ou de licenciement (pour faute grave ou non) sont toujours délicates et sources de difficultés. La procédure sera analogue à celle à prévoir pour l'absence non planifiée. De plus, la procédure devra préciser la bonne fin à donner aux messages destinés au travailleur licencié et aux fichiers professionnels et privés stockés sur le poste de travail. Ici aussi l’accès se fera avec prudence et de manière « progressive », par exemple en triant sur les objets ou d’autres critères avant de prendre connaissance du contenu.