

**DELIBERATION N° 2012-119 DU 16 JUILLET 2012 DE LA COMMISSION DE CONTROLE DES
INFORMATIONS NOMINATIVES PORTANT RECOMMANDATION SUR LES TRAITEMENTS
AUTOMATISES D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE
« *GESTION DE LA MESSAGERIE PROFESSIONNELLE* »
UTILISES A DES FINS DE CONTROLE DE L'ACTIVITE DES EMPLOYES**

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, et son protocole additionnel ;

Vu la Recommandation du Conseil de l'Europe n° R (89) 2 du 19 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Vu la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;

Vu la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières ;

Vu la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives ;

Vu le Code civil, et notamment son article 989 ;

Vu les articles 341 et suivants du Code pénal relatifs à la violation du secret des correspondances ;

Vu l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, susvisée ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

La Commission de Contrôle des Informations Nominatives,

Conformément à l'article 1^{er} alinéa 1 de la loi n° 1.165 du 23 décembre 1993, modifiée, les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution.

La Commission de Contrôle des Informations Nominatives, Autorité Administrative Indépendante, a pour mission de veiller au respect de ces dispositions. A ce titre, elle est notamment habilitée à formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par la loi.

Par la présente recommandation, la Commission souhaite préciser les grands principes de protection des informations nominatives applicables aux traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » mis en œuvre sur le lieu de travail par l'employeur, et utilisé notamment à des fins de contrôle de l'activité des employés.

Cette recommandation a ainsi vocation à orienter les responsables de traitement dans leurs démarches auprès de la Commission.

I. Remarques liminaires

A l'heure actuelle, la messagerie professionnelle est devenue un outil incontournable et bien souvent nécessaire à l'accomplissement, par l'employé, de ses missions de travail.

La banalisation d'un tel dispositif de communication électronique sur le lieu de travail ne l'exonère pas pour autant des dispositions de la loi n° 1.165, modifiée. En effet, l'exploitation d'une messagerie professionnelle implique la mise en œuvre sous-jacente d'un traitement automatisé d'informations nominatives, au sens de l'article 1^{er} de ladite loi.

La messagerie professionnelle peut être utilisée de manière tout à fait ordinaire, pour l'envoi et la réception de correspondances électroniques. Or comme l'a invariablement affirmé la Cour européenne des droits de l'homme, appliquant l'article 8 de la Convention de sauvegarde des droits de l'homme (CESDH), le droit au respect de la vie privée et au secret des correspondances s'étend au lieu de travail.

Ce droit est toutefois susceptible de connaître des limitations justifiées par le respect d'intérêts légitimes de l'employeur. Dans ce cadre, ce dernier peut en effet décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie mise à la disposition de ses employés.

Entrent alors en conflit deux intérêts apparemment contradictoires, mais néanmoins conciliables. Il convient donc de rechercher le juste équilibre entre les droits des employés et ceux de l'employeur.

A ce titre, la Commission rappelle tout d'abord qu'il est préférable d'opter pour une politique de prévention plutôt que de répression.

Par ailleurs, elle appelle l'attention du responsable de traitement sur la nécessité de responsabiliser ses employés à la protection de leurs informations nominatives.

Enfin, elle rappelle que la messagerie personnelle de l'employé ne pourra, quant à elle, faire l'objet d'aucune surveillance ni d'aucun contrôle nominatif.

Au vu de ces éléments, la Commission estime nécessaire de retenir les principes fondamentaux ci-après exposés.

II. Champ d'application et formalités légales applicables

Les principes consacrés par la présente délibération s'appliquent à tout traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* », mis en œuvre sur le lieu de travail ou dans le cadre d'activités professionnelles par le responsable de traitement ou son représentant, au sens de l'article 24 de la loi n° 1.165, modifiée.

➤ **Régimes applicables aux traitements ordinaires**

Dans le cadre d'une exploitation ordinaire des messageries professionnelles, c'est-à-dire en l'absence de contrôle ou de surveillance nominative de ces dernières, la Commission rappelle que le traitement est soumis à déclaration, dès lors qu'il est mis en œuvre par un responsable de traitement, personne physique ou morale de droit privé, en application de l'article 6 de la loi n° 1.165, modifiée.

Concernant les responsables de traitement relevant de l'article 7 de la loi n° 1.165, modifiée, ces traitements sont soumis à l'avis préalable de la Commission.

➤ **Régimes applicables aux traitements utilisés à des fins de surveillance ou de contrôle de l'activité des employés**

Si la messagerie est utilisée par l'employeur « *à des fins de surveillance* » ou dans le cadre de « *souçons d'activités illicites* », le traitement est alors soumis à l'autorisation préalable de la Commission, conformément à l'article 11-1 de la loi n° 1.165, susvisée, dès lors que cette surveillance vise des individus déterminés ou déterminables, au sens de l'article 1^{er} de ladite loi.

Ce régime est applicable aux personnes physiques ou morales de droit privé. Les « *personnes morales de droit public, autorités publiques* » visées par l'article 7, précité, demeurent soumises au régime de la demande d'avis.

➤ **Personnes concernées**

Les personnes concernées par ce type de traitements sont l'ensemble des expéditeurs et destinataires des communications électroniques échangées par le biais de la messagerie professionnelle mise à la disposition des employés par le responsable de traitement ou son représentant.

Cela inclut tant les employés susmentionnés, quelle que soit la nature de leur emploi (salarié, consultant en mission, etc.), que les tiers sans lien de subordination avec le responsable de traitement ou son représentant.

III. Protection des correspondances privées sur le lieu de travail

La Commission rappelle que 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* ».

Elle relève par ailleurs que dans un arrêt NIEMIETZ C. ALLEMAGNE en date du 16 décembre 1992, la Cour Européenne des Droits de l'Homme a consacré le droit au respect de la vie privée sur le lieu de travail.

Elle affirme en effet qu'il serait « *trop restrictif de la limiter à un « cercle intime » où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales* ».

La Commission considère que le respect du secret des correspondances privées est un principe immuable. Ainsi, l'employeur ne peut en aucun cas accéder aux contenus des messages privés de son employé envoyés ou reçus à partir de la messagerie professionnelle mise à sa disposition par l'employeur – et *a fortiori* depuis une messagerie personnelle.

Cela implique qu'aient été au préalable définies, dans la charte d'usage des outils de communication électronique mentionnée au point VII, les modalités permettant aux employés d'identifier les messages privés adressés depuis la messagerie professionnelle, par exemple par l'adjonction de mots clés dans l'objet du message tels que « *privé* », « *[PRV]* », « *personnel* ».

Dans le cas où l'employeur interdirait tout usage de la messagerie professionnelle à des fins privées, celui-ci ne saurait pour autant s'exonérer du principe de respect de la vie privée et du secret des correspondances. Il ne pourra donc accéder à aucun message identifié comme « *privé* » ou « *personnel* ».

Enfin, la Commission souhaite souligner que seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés, et cela même s'il a des motifs légitimes de suspecter des actes de concurrence déloyales 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. En tout état de cause, l'employeur ne peut en aucun cas prendre l'initiative d'accéder auxdits messages.

IV. Licéité du traitement

➤ Principe de proportionnalité : contrôle gradué des messageries

Conformément à l'article 11-1 de la loi n° 1.165, modifiée, les traitements ayant pour finalité « *Gestion de la messagerie professionnelle* » utilisés à des fins de surveillance ou de contrôle de l'activité des employés doivent, pour être licites, être « *nécessaires à la poursuite d'un objectif légitime essentiel et [respecter] les droits et libertés mentionnés à l'article premier des personnes concernées (...)* ».

A ce titre, la Commission considère tout d'abord qu'il revient au responsable de traitement, ou à son représentant, de mettre en place une procédure de contrôle adaptée au niveau de risque auquel il est confronté. Ainsi, les mesures prises doivent être strictement nécessaires au but recherché.

Par ailleurs, outre les diverses mesures techniques et organisationnelles préventives (ex. mécanisme de blocage ou d'alerte visible des employés), il lui appartient de mettre en place, en fonction du but recherché, une procédure de contrôle graduée, à savoir :

- Phase 1 :** le contrôle non nominatif global des fichiers journaux de la messagerie (ex. nombre de messages envoyés, format des pièces jointes, volumes, etc.) ;
- Phase 2 :** le contrôle des fichiers journaux des messageries d'un ou plusieurs employés déterminés ;
- Phase 3 :** le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés ou déterminables, sélectionnés aléatoirement (échantillonnage) ou par filtrage automatique ;
- Phase 4 :** le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés.

Afin de respecter le principe de proportionnalité, la Commission recommande la mise en place de procédures de contrôle comme suit :

Tout d'abord, elle rappelle que seules les phases 1 et 2 sont justifiées pour assurer la sécurité du réseau informatique et garantir son bon fonctionnement, ainsi que pour détecter tout abus d'usage de la messagerie au regard des règles internes posées par le responsable de traitement ou son représentant.

Dans ce cadre, la Commission demande à ce que le contrôle débute par la phase 1. Si des anomalies sont constatées, elle recommande à ce que les employés soient avertis qu'en cas de nouvelles anomalies de même nature, un contrôle individualisé aura lieu (phase 2).

Dans le cas où une obligation légale ou réglementaire le justifie, comme visée au point IV de la présente délibération, le responsable de traitement ou son représentant peut mettre en place une procédure de surveillance préventive (phase 3). Dans ce cas, le contrôle doit s'opérer à intervalles réguliers (ex. mensuellement) et de manière aléatoire afin de ne pas conduire à une surveillance permanente d'un ou plusieurs salariés en particulier. Cela peut également prendre la forme d'un système de filtrage automatique de contenus permettant l'envoi d'alertes en fonction des occurrences de mots clés détectés.

Enfin, à l'occasion des phases 2 ou 3, ou au vu d'autres éléments autrement portés à sa connaissance, le responsable de traitement ou son représentant peut soupçonner l'existence d'une violation grave de ses intérêts économiques, commerciaux ou financiers, de faits susceptibles d'engager sa responsabilité civile ou pénale, ou encore de faits illicites commis par un ou plusieurs employés.

Dans ce cas, il pourra passer à la phase 4, dès lors que ce contrôle est strictement nécessaire aux fins de rassembler des éléments de preuve, notamment en vue d'une procédure disciplinaire et/ ou judiciaire.

Il conviendra alors de définir une procédure stricte afin de garantir le respect des droits du ou des employés visés, notamment leur droit à la vie privée et au secret des correspondances, tel que visés au point III de la présente délibération.

Enfin, la Commission rappelle que d'une manière générale, toute surveillance nominative permanente est interdite.

➤ **Cas particulier du contrôle ou de la surveillance des messageries professionnelles mis en œuvre par une autorité publique ou pour son compte**

Conformément à l'article 8§1 de la CESDH, « *Toute personne a droit au respect de sa vie privée (...) de sa correspondance* ».

Dans un arrêt COPLAND C. ROYAUME-UNI du 3 avril 2007, la Cour européenne des droits de l'homme indique en outre que « *la collecte et la conservation (...) de données à caractère personnel se rapportant à l'usage (...) du courrier électronique (...) [constitue] une ingérence dans l'exercice du droit de l'intéressé au respect de sa vie privée et de sa correspondance, au sens de l'article 8* ».

Dans sa délibération n° 2011-82 du 21 octobre 2011 portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives, la Commission rappelle les conditions de licéité prévues par l'article 8§2 de la CESDH, telles qu'interprétées et précisées par une jurisprudence constante de la Cour.

Elle relève que « *la Cour Européenne est très exigeante en ce qui concerne les mesures de surveillance des personnes, telles que (...) le contrôle de la correspondance écrite ou orale (...)* ».

Ainsi, la Commission rappelle en premier lieu que toute surveillance ou contrôle, par une autorité publique ou pour son compte, d'une messagerie professionnelle, ne peut être licite que si cela est prévu par un texte conforme à l'ordre juridique interne définissant avec une précision suffisante, notamment, les conditions de la collecte des données, ainsi que leurs modalités d'exploitation.

En second lieu, la Commission rappelle que conformément à l'article 8§2 de la CESDH, la mise en place de mesures de surveillance ou de contrôle doit être strictement « *nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

V. Justification du traitement

En application de l'article 10-2 de la loi n° 1.165, modifiée, la Commission considère qu'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » peut être justifié par :

➤ **Le respect des obligations légales des établissements bancaires et assimilés**

La Commission prend acte des obligations particulières de vigilance ainsi que de traçabilité des opérations financières imposées aux établissements bancaires ou assimilés, notamment par les textes suivants :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application ;

- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;
- l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers.

Ainsi, la Commission estime qu'afin de respecter leurs obligations, ces responsables de traitement ou leurs représentants peuvent mettre en place des procédures de surveillance ou de contrôle des messageries professionnelles, dans le strict respect des principes définis par la présente délibération, notamment les principes de proportionnalité et de transparence, définis aux points III et VI.

➤ ***La réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou son représentant***

La Commission considère qu'une procédure de surveillance ou de contrôle des messageries professionnelles peut être justifiée par un intérêt légitime du responsable de traitement ou de son représentant, tel que :

- la sécurité et le bon fonctionnement technique du réseau ou système informatique ;
- le contrôle du respect des règles internes d'usage des outils de communication électronique, du règlement intérieur, (...);
- la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;
- la protection contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice ;
- la prévention de faits illicites.

A défaut de surveillance, si le traitement est exploité uniquement à des fins ordinaires, la Commission considère qu'il peut être justifié par l'intérêt légitime de l'employeur de permettre l'optimisation de l'accomplissement des missions de travail de ses employés.

Enfin, la Commission rappelle qu'eu égard à l'existence d'un lien de subordination ou d'un lien contractuel entre employeur et employé, le consentement de ce dernier, lequel doit être libre, spécifique et éclairé, ne peut jamais constituer une justification à la mise en œuvre de ce type de traitement.

VI. Fonctionnalités du traitement

La Commission considère que compte tenu du caractère intrinsèquement intrusif des procédures de contrôle ou de surveillance nominative des messageries professionnelles, la mise en œuvre de traitements automatisés y afférents ne peut avoir d'autres fonctionnalités que de :

- répondre à une obligation légale ;
- garantir le respect d'un intérêt légitime du responsable de traitement ou de son représentant, tel que visé au point IV de la présente délibération ;
- permettre la constitution de preuves en cas de violation de ces intérêts, ou en cas d'infractions civiles ou pénales.

Au-delà des fonctionnalités susmentionnées, la Commission rappelle que dans le cadre de son exploitation ordinaire, un traitement automatisé ayant pour finalité « *Gestion*

de la messagerie professionnelle » est susceptible d'avoir, notamment, les fonctionnalités suivantes :

- échange de messages électroniques en interne ou avec l'extérieur ;
- historisation des messages électroniques entrants et sortants ;
- gestion des contacts de la messagerie électronique ;
- gestion des dossiers de la messagerie et des messages archivés ;
- établissement et lecture de fichiers journaux ;
- gestion des habilitations d'accès à la messagerie ;
- interconnexion avec l'agenda.

VII. Information de la personne concernée

La Commission rappelle que conformément aux dispositions de l'article 14 de la loi n° 1.165, modifiée, les personnes concernées par l'exploitation de leurs informations nominatives doivent être informées, par tout moyen qu'il appartient au responsable de traitement ou à son représentant de déterminer, de :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'accès et de rectification aux informations les concernant.

En cas de surveillance ou de contrôle de la messagerie professionnelle, la Commission appelle l'attention du responsable de traitement sur le fait qu'une telle obligation d'information relève également d'un souci de transparence envers les employés, ainsi que de loyauté dans la relation de travail.

A cet égard, elle demande à ce que le responsable de traitement ou son représentant mette en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les procédures de contrôle et de surveillance mises en œuvre, suivant les règles posées au point III de la présente délibération ;
- la ou les finalités de ces procédures ;
- les personnes habilitées à avoir accès au traitement ;
- la durée de conservation des données collectées ;
- les modalités d'exercice par les personnes de leurs droits d'accès à leurs données.

En outre, afin de limiter l'atteinte portée à la vie privée des employés, la Commission demande au responsable de traitement ou à son représentant de définir dans la charte susmentionnée :

- si l'usage de la messagerie professionnelle est toléré à des fins privées, et dans l'affirmative, les modalités d'identification des messages privés ;
- la procédure d'accès à la messagerie professionnelle par des personnes habilitées, en cas d'absence temporaire ou définitive de l'employé, et ce afin d'assurer la continuité des activités.

Enfin, 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.

VIII. Catégories d'informations traitées

Conformément aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée, la Commission considère que les catégories d'informations suivantes peuvent être collectées et traitées :

- identité : nom, prénom, identifiant ;
- messages : contenu, objet, dossiers de classement ou d'archivage ;
- gestion des contacts : nom, prénom, raison sociale, (...) ;
- informations temporelles : date, heure ;
- données d'identification électronique : adresse de messagerie électronique ;
- logs d'accès : logs de connexion des personnels habilités à avoir accès au traitement ;
- fichiers journaux : 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, historisation des habilitations.

IX. Personnes ayant accès aux informations et les destinataires

La Commission considère que l'accès aux informations objets du traitement doit être limité aux seules personnes qui, dans le cadre de leurs attributions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement ou du but recherché. Ces accès devront être définis dans la charte mentionnée au point VI de la présente délibération.

En ce qui concerne les traitements visés aux articles 11 et 11-1 de la loi n° 1.165, modifiée, elle rappelle que conformément aux dispositions de l'article 17-1 de ladite loi, le responsable de traitement ou son représentant doit « *déterminer nominativement la liste de personnes autorisées qui ont seules accès, pour les strictes besoins de l'accomplissement de leurs missions, aux locaux et aux installations utilisés pour les traitements, de même qu'aux informations traitées* ».

Enfin, la Commission rappelle que les autorités judiciaires et administratives peuvent, dans le cadre exclusif des missions qui leur sont légalement conférées, être rendues destinataires de données objets du traitement, notamment pour la recherche de preuves ou la constatation d'infractions.

Dans ce cas, des mesures de sécurité particulières devront être prises, concernant notamment le support sur lequel ces informations sont transmises, ainsi que la procédure de transfert, conformément aux dispositions du point IX de la présente délibération.

X. Confidentialité et mesures de sécurité

La Commission rappelle qu'en application des articles 17 et 17-1 de la loi n° 1.165, modifiée, le responsable de traitement ou son représentant doit prendre toutes mesures utiles pour préserver la sécurité des informations objets du traitement, telles que l'authentification par un identifiant et un mot de passe individuel (réputé fort), régulièrement renouvelés.

Par ailleurs, les accès des personnes mentionnées au point VIII devront faire l'objet d'une journalisation.

La Commission demande en outre à ce que les personnes habilitées à avoir accès au traitement, et notamment au contenu des messages électroniques professionnels, soient astreintes à une obligation de confidentialité particulièrement stricte.

Enfin, elle admet que des données puissent être extraites et/ou copiées sur un support distinct en vue d'une communication aux autorités administratives ou judiciaires légalement habilitées. Elle rappelle que dans ce cas, toute copie ou extraction de ces données devra être chiffrée sur son support de réception.

XI. Durée de conservation

La Commission rappelle que conformément à l'article 10-1 de la loi n° 1.165, modifiée, les informations nominatives objets du traitement 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 énumérées au point V de la présente délibération, la Commission distingue trois hypothèses :

1. si la messagerie est exploitée de manière ordinaire, la Commission estime qu'une durée de conservation maximale de 1 an est suffisante ;
2. si la messagerie est utilisée à des fins de contrôle ou de surveillance de l'activité des employés, une durée de conservation maximale de 5 ans est suffisante. Cela correspond au délai de prescription en matière prudhomme (article 2092 bis du Code civil) ;
3. si le contrôle a pour but la détection de crimes ou délits visés aux articles 218-1 et 218-2 du Code pénal, la durée de conservation pourra être au maximum de 10 ans, conformément au délai de prescription prévu à l'article 12 du Code de procédure pénale.

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, conformément à l'article 10-1 susvisé.

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

Après en avoir délibéré,

Rappelle que :

- l'exploitation d'une messagerie professionnelle implique la mise en œuvre d'un traitement automatisé d'informations nominatives, au sens de l'article 1^{er} de la loi n° 1.165, modifiée ;
- tous les traitements ainsi exploités devront remplir les conditions fixées par la loi n° 1.165 du 23 décembre 1993, modifiée, telles que précisées dans le cadre de la présente délibération.

Le Président,

Michel Sosso